matemática moderna

Papy

V

EDITORIAL UNIVERSITARIA DE BUENOS AIRES

MATEMÁTICA MODERNA

GEORGES PAPY

"La matemática que, a principio de siglo, apenas tenía aplicación fuera de la física y del arte del ingeniero, se ha convertido en elemento fundamental del humanismo contemporáneo y en herramienta indispensable en la mayoría de los dominios del pensamiento, de la ciencia y de la técnica", sostiene el autor del presente libro, y de este hecho innegable deduce la necesidad de enseñar los principios matemáticos básicos a todos los estudiantes secundarios.

Matemática moderna es una obra destinada a profesores y alumnos de la escuela media, pero útil a todos quienes busquen una versión actual de la ciencia. En su lengua original ha llegado ya a los seis volúmenes, inmediatamente traducidos a otros idiomas. Este quinto tomo que presenta EUDEBA se ocupa de los siguientes temas: combinatoria, la aritmética de los números enteros racionales, más alto común divisor, más bajo común múltiplo, factorizaciones primas de números naturales, la aritmética de los números racionales, anillos conmutativos y cuerpos, propiedades aritméticas de los grupos y cuerpos de Galois. Cada uno de ellos

MATEMÁTICA MODERNA

5

ARITMÉTICA

LA ESCUELA EN EL TIEMPO
Textos del secundario/Matemática

PAPY
con la colaboración de
Frédérique Papy

MATEMATICA MODERNA

Tomo V

EDITORIAL UNIVERSITARIA DE BUENOS AIRES

Título de la obra original:
Mathématique moderne
Marcel Didier, Editeur, Bruxelles, Paris, 1966

Traducida por
Estela O. de González Baró

La revisión técnica estuvo a cargo de la traductora

EN EL AÑO DEL SESQUICENTENARIO
DE LA FUNDACION
DE LA UNIVERSIDAD DE BUENOS AIRES

© 1971
EDITORIAL UNIVERSITARIA DE BUENOS AIRES
Rivadavia 1571/73

Sociedad de Economía Mixta
Fundada por la Universidad de Buenos Aires

Hecho el depósito de ley
IMPRESO EN LA ARGENTINA – PRINTED IN ARGENTINA

A Louis Bouckaert

PREFACIO

Esta obra, destinada a alumnos de 14 a 18 años, abarca la aritmética de la escuela secundaria.

Además de los problemas de numeración (libro 1), la aritmética estudia el anillo de números enteros racionales (libro 2), de su cuerpo de fracciones Q, +, · (libro 3), de sus anillos y cuerpos cocientes Z_n, +, · (libro 4).

Se impone una primera teoría de anillos conmutativos y cuerpos, que completa el libro 4.

El libro 5 aplica los grandes teoremas de los libros 1, 2, 4. Los resultados concernientes al orden de los elementos y de los subgrupos de un grupo, conducen a un último y breve capítulo sobre los cuerpos finitos.

* * *

El libro **1** *desarrolla las ideas esbozadas en un artículo de* Matemática y Pedagogía *y ha sido objeto, en una versión anterior, de una edición policopiada por el Centro Belga de Pedagogía de la Matemática*[1].

La presente redacción tiene en cuenta la enseñanza que hicimos de la combinatoria en los cursos de alumnos de 15 años, durante los últimos siete años.

* * *

En la óptica moderna, la combinatoria es esencialmente el problema de la enumeración de las aplicaciones, inyecciones y biyecciones de un conjunto finito en un conjunto finito.

Este estudio sólo requiere el conocimiento de reglas elementales de cálculo con números naturales, y puede encararse muy temprano. Sin embargo, hay que evitar que la enumeración se vuelva una manía fastidiosa y acaparadora.

---

1. PAPY: *Analyse Combinatoire* – Mathematica et Paedagogia – nº 16, pp. 6 a 10, Bruselas 1958–59
   Ver también
   HOLVOET, la misma revista – nº 21, pp. 6 a 31, 1961.
   PAPY: *Vectoriel euclidien plan, Analyse Combinatoire*, Centro Belga de Pedagogía de la Matemática, 1964.

Sugerimos realizar esta enseñanza en la clase de 14 a 15 años comenzando, de una manera no sistemática, por ejercicios de enumeración, al iniciar el estudio de conjuntos y relaciones.

Los temas desarrollados en el libro 1 han sido seleccionados teniendo en cuenta las necesidades de los utilizadores, sobre todo en los cursos de Probabilidad y de Física matemática de los dos primeros años de la Universidad. Las fórmulas importantes del libro 1 se aplican en los libros 4 y 5 de esta obra.

La exposición respeta siempre la visión global de la situación. Evita las demostraciones artificiales por recurrencia, que constituyen un formalismo pesado y pernicioso.

El libro 1 no introduce ninguna noción nueva para los alumnos, ya familiarizados con los conceptos conjuntistas y relacionistas (de la manera como se exponen en [MM1]). Sólo comprende la definición de factorial. Se rechazan deliberadamente las anticuadas denominaciones de arreglo, combinación, agrupamiento simple o con repetición,... que hacen una doble utilización de nociones más claras, más generales y en adelante inevitables de la matemática moderna. De este modo, la combinatoria deja así de aparecer como un tema separado del resto de la matemática.

La materia del libro 1 es naturalmente fértil en problemas que interesan mucho a los alumnos y cuyas respuestas muchas veces los asombran. En la elección que el lector puede hacer de tales problemas, nunca perdimos de vista las aplicaciones reales.

* * *

El libro 2 (Cap. 2 a 5) desarrolla las ideas que esbozamos en un artículo de Mathematica et Paedagogia[1] *y que expusimos de manera bastante diferente en un capítulo de* Groupes[2].

Este libro fue totalmente enseñado en una clase de 3º científica (alumnos de 15 años) y la presente redacción tiene en cuenta esta experiencia.

* * *

La teoría de enteros racionales, que continúa siendo el alma de la aritmética, debe seguir, en su presentación, la misma evolución que la teoría de los ideales que la generaliza. Siendo esencialmente multiplicativa en sus orígenes,

---

1. PAPY: Mathematica et Paedagogia, nº 8, pp. 6 a 19, Bruselas 1959.
   Ver también un artículo de YOLANDE ROCH en la misma revista, nº24, pp. 51 a 56, 1963.

2. PAPY: *Grupes*, Ed. Universitarias de Bruselas, Bruselas; Dunod, París, 1961, Cap. 6.

esta teoría se vuelve fundamentalmente aditiva bajo el impulso de Emmy Noether, que realizó así la linealización de la teoría.

En el estudio del anillo Z, +, · las combinaciones lineales tienen necesariamente coeficientes enteros racionales. El conjunto de combinaciones lineales de elementos de una parte P de Z es el menor subgrupo de Z,+ que contiene P. El estudio de los subgrupos de Z, + y en particular del subgrupo engendrado por una parte P de Z, es el punto de partida más natural del libro 2.

El capítulo 2 demuestra el teorema fundamental de la aritmética:

"Todo subgrupo de Z, + es cíclico (y está engendrado por uno y sólo uno de sus naturales)". La ciclicidad es uno de los leitmotiv de esta obra.

El aspecto multiplicativo de la teoría hace su aparición en el capítulo 3 con la introducción de la relación "divide". Como la relación "divide" está incluida en la relación "menor que" mientras uno se limita a los naturales no nulos, a menudo se confunden horriblemente las dos nociones que evitamos, principalmente, con un ligero cambio terminológico que se inspira en el ejemplo anglo-sajón.

El más alto común divisor de un conjunto P de números enteros racionales es el generador natural del subgrupo engendrado por P, y es, por lo tanto, una combinación lineal, con coeficientes enteros racionales, de elementos de P (relación llamada de Bezout).

A partir de este resultado fundamental –inaccesible a los que se encierran en el conjunto de números naturales– se llega fácilmente a las factorizaciones primas (Cap. 4).

El capítulo 5 pone en evidencia el reticulado distributivo ω, $\wedge$, $\vee$. STONE demostró, en 1934, que todo reticulado distributivo complementado es isomorfo a un reticulado de partes de un conjunto. Se ve que está de acuerdo con la naturaleza profunda de las cosas, el exhibir un isomorfismo de ω, $\wedge$, $\vee$ sobre el reticulado constituido por los conjuntos de divisores primarios de los números enteros naturales... y deducir las propiedades de ω, $\wedge$, $\vee$. La suerte que corren así los divisores primarios está de acuerdo con la importancia de los ideales primarios en la teoría de los anillos de Noether.

* * *

Sugerimos enseñar el libro 2 en las clases de 15 a 16 años.

El conocimiento de la aritmética de los números enteros racionales que los alumnos tendrán que poseer, está condensado en 6 sorprendentes teoremas. La teoría se apoya en 30 proposiciones, puestas en evidencia con el fin de obtener una mayor claridad. Es inútil retenerlas, puesto que se deducen fácilmente de los teoremas (de los cuales las proposiciones son generalmente fragmentos provisorios).

* * *

El libro 3 *–la aritmética de los números racionales– no es esencial, y no se considerará en lo sucesivo. Sin embargo, constituye una interesante aplicación del libro 2, y pone en evidencia la posibilidad de desarrollar una teoría de la divisibilidad en un cuerpo. Algunos de los resultados obtenidos son bastante inesperados.*

La teoría desarrollada en el único capítulo de dicho libro continúa siendo totalmente válida en el cuerpo de fracciones de todo anillo principal y en particular en el cuerpo R(X) de "funciones" racionales reales. Esta teoría se utiliza sobre todo en el cálculo de primitivas.

Las congruencias y los teoremas de Fermat y Wilson –temas tradicionales de los cursos de aritmética– encuentran ubicación natural en la teoría de los anillos de restos Z_n, $+$, $\cdot$ *(Cap. 7). Este estudio enriquece considerablemente el horizonte de los alumnos y les revela situaciones nuevas.*

El teorema de Fermat se prueba de manera muy elemental. En el capítulo 12 se da una generalización fundada en el teorema de Lagrange.

A esta altura, los alumnos conocen tal número de anillos conmutativos y cuerpos, que se impone la realización de una teoría muy elemental (Cap. 8). Este capítulo da lugar al anillo de aplicaciones de un conjunto en un anillo, y proporciona así un método de fabricación de nuevos anillos.

El capítulo 9 estudia el anillo de funciones polinomios de un anillo. Sin abordar la teoría de polinomios abstractos se muestra –consecuencia de la fórmula de Fermat– que en el cuerpo Z_p, *polinomios formales distintos definen la misma función polinomio.*

La teoría de la divisibilidad por $x - a$ *establece que toda función polinomio no nula admite un número finito de raíces. Luego resulta el teorema de Wilson y el hecho de que, sobre un cuerpo infinito, dos polinomios formales distintos definen funciones polinomios diferentes.*

Sugerimos enseñar el libro 4 (Cap. 7 a 9) en la clase de 16 años.

El libro 5 (Cap. 10 a 12) utiliza esencialmente resultados fundamentales de los libros 1, 2 y 4.

El capítulo 10 estudia propiedades elementales de los subgrupos de un grupo y de sus clases laterales. También establece el teorema de divisibilidad de Lagrange.

Las propiedades aritméticas del orden de los elementos de un grupo constituyen el objeto del capítulo 11.

El libro termina con un estudio breve pero sugestivo de los cuerpos finitos. Se establece la ciclicidad del grupo multiplicativo de todo cuerpo finito, y se demuestra que toda transformación de un cuerpo tal es una función polinomio.

⁂

El libro 5 está particularmente destinado a los alumnos de los últimos cursos secundarios que se preparan para seguir estudios de matemática.

⁂

Como de costumbre, tengo el agradable deber de rendir un afectuoso homenaje a Frédérique, que supo imponerme una disciplina estricta, sin la cual jamás habría terminado esta obra. Frédérique que tuvo, además, el gran mérito de mantener esta exposición de la Aritmética dentro de límites aceptables.

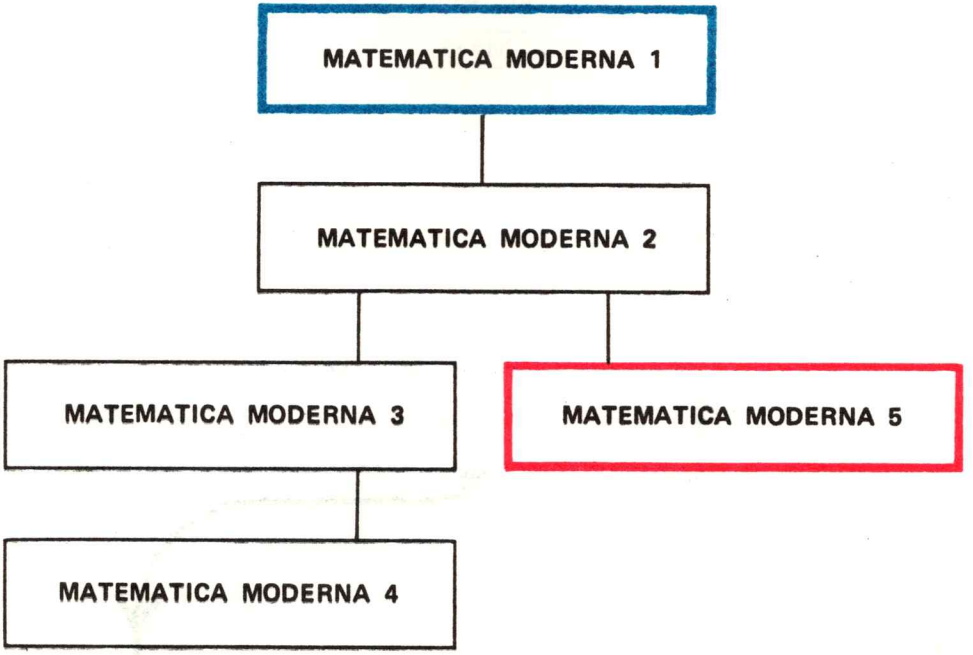
El capítulo 1 mejoró enormemente con las acertadas observaciones enviadas por mis colegas el profesor Robert BALLIEU de la Universidad de Lovaina y el profesor Jean TEGHEM de la Universidad de Bruselas. Los problemas de análisis combinatorio fueron elegidos teniendo en cuenta indicaciones del señor Jean REIGNIER, profesor en la Universidad de Bruselas, quien nos indicó cuáles eran las situaciones que se presentan efectivamente en los cursos de candidatura de Física Matemática. Expreso a los tres mi amistosa gratitud.

Mi reconocimiento también se dirige a la señora Gilberte CAPIAUX y a las señoritas Irma DUMRAUF y Nimet ENUNLU, asistentes del Centro Belga de Pedagogía de la Matemática, establecieron el índice y corrigieron las pruebas con minucioso empeño.

La señora Georgette CAGNANT, que consagró su habitual talento a los dibujos que ilustran este libro, y la señorita Françoise JASSOGNE, autora de la tapa, tienen derecho a nuestro agradecimiento.

PAPY
Duinbergen, agosto de 1965

ADVERTENCIA



MM1 presenta el cuadro y el lenguaje de la matemática actual. Conocer las nociones conjuntistas, relacionistas y de grupos estudiadas en MM1 para seguir toda exposición moderna de matemática, y en particular para abordar MM2, MM3, MM4, MM5

MM2 introduce principalmente la estructura numérica más importante de la matemática, el **cuerpo totalmente ordenado, arquimedeano completo de números reales.**

MM3 se ocupa de geometría métrica plana

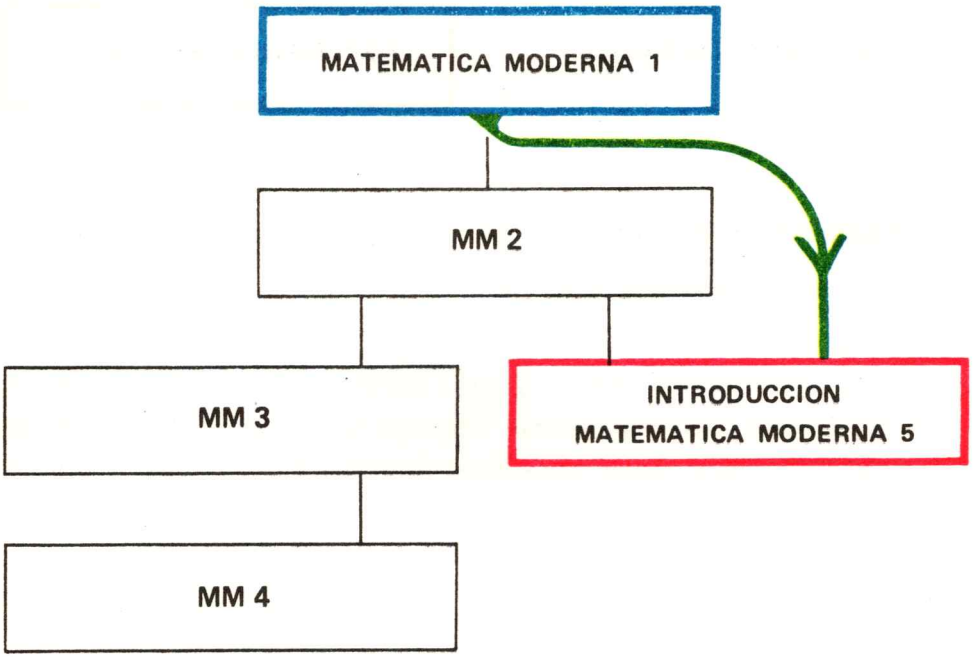
MM4 estudia las funciones de **R** en **R**

MM5 no se apoya para nada sobre MM3 ni sobre **MM4**

Para abordar y comprender MM5 basta conocer MM1 y MM2

¡Pero ello tampoco es indispensable!

Pensamos que resultaría agradable al lector hallar en una INTRODUCCION, las nociones relativas al anillo ordenado Z , + , · , ⩽ que son las únicas que interesa conocer para abordar MM5



Introducción

Para abordar MM5 además de las nociones expuestas en MM1 basta saber que

$\mathbf{Z},\ +,\ \cdot\ ,\ \leqslant$

es un

anillo conmutativo, totalmente ordenado, arquimedeano

Conviene explicar qué se entiende por eso.

NUMEROS ENTEROS RACIONALES

Z *es el conjunto de (números)* **enteros racionales**

$$\mathbf{Z} = \{0,\ 1,\ -\ 1,\ 2,\ -\ 2,\ \ldots\}$$

ANILLO CONMUTATIVO

$\mathbf{Z},\ +,\ \cdot$

es un

anillo conmutativo

significa

Z *está provisto de las leyes internas totalmente definidas* $+$ *y* $\cdot$

$\mathbf{Z},\ +$ *es un grupo conmutativo.*

- $\cdot$ *es asociativa y conmutativa*
- $\cdot$ *distribuye* $+$

El anillo Z, +, · satisface la regla de los signos

Si	$a,\ b \in \mathbf{Z}$
Entonces	$(-a)\ b = -(a\ b) = a(-b)$
	$(-a)\ (-b) = ab$

REGLA DE LOS SIGNOS

ORDEN TOTAL

Z, $\leqslant$ *es un* **ordenado total**

$\ldots < -5 < -4 < -3 < -2 < -1 < 0 < 1 < 2 < 3 < 4 < 5 < \ldots$

Todas las nociones recordadas hasta aquí han sido introducidas en MM1 **al cual enviamos eventualmente al lector.**

GRUPO TOTALMENTE ORDENADO

Z, +, $\leqslant$ *es un* **grupo totalmente ordenado**

significa

Z, + *es un grupo conmutativo*

Z, $\leqslant$ *es un ordenado total*

$\forall\ x, y, z \in \mathbf{Z}$: $x \leqslant y \Longrightarrow x + z \leqslant y + z$

ANILLO CONMUTATIVO TOTALMENTE ORDENADO

$Z, +, \cdot, \leqslant$

es un

anillo conmutativo totalmente ordenado

significa

$Z, +, \cdot$ *es un anillo conmutativo*

$Z, +, \leqslant$ *es un grupo conmutativo ordenado*

$\forall x, y \in Z \quad : \quad (o \leqslant x \quad \text{y} \quad o \leqslant y) \Longrightarrow o \leqslant xy$

ANILLO CONMUTATIVO TOTALMENTE ORDENADO ARQUIMEDEANO

$Z, +, \cdot, \leqslant$

es un

anillo conmutativo totalmente ordenado arquimedeano

significa

$Z, +, \cdot, \leqslant$ *es un anillo conmutativo totalmente ordenado*

tal que

Si $a \in Z \quad \text{y} \quad o < b \in Z$

Entonces $\exists!\, q \in Z, \exists!\, r \in Z \quad : \quad a = bq + r \quad con \quad o \leqslant r < b$

CUANTIFICADORES

Los **cuantificadores** A, E, E! son utilizados en esta obra como simples abreviaturas estenográficas.

$\forall$ se lee "para todo"

$\exists$ se lee "existe"

$\exists!$ se lee "existe uno y sólo uno"

LIBRO 1

COMBINATORIA

1

Combinatoria

1 — PROBLEMA

— Escribe todas las "palabras" de dos letras (que tengan o no sentido) que empiecen con consonante y terminen en vocal.

— b a , b e , b i , b o , b u , b y
c a , c e , c i , c o , c u , c y
d a , d e , . . .
. . .
. . . , x i , x o , x u , x y
z a , z e , z i , z o , z u , z y

— ¿Cuántas de esas palabras escribiste?

— 20 × 6 = 120

— Hay tantas de esas palabras, como cuplas cuyo origen es una consonante y cuya extremidad es una vocal.

Si C designa el conjunto de consonantes y V el conjunto de vocales

Entonces el número que buscamos es # (C × V)

En virtud de la definición de multiplicación : #(C × V) = # C · # V

Y por lo tanto el número que buscamos es

#(C × V) = # C · # V = 20 · 6 = 120

4

EJERCICIOS

1. ¿Cuántas "palabras" de dos letras que empiecen con vocal y terminen en consonante puedes formar?

2. ¿Cuántas "palabras" de dos letras que empiecen y terminen en consonante puedes formar?

3. ¿Cuántas "palabras" de dos letras que empiecen y terminen en vocal?

4. ¿Cuántas "palabras" de dos letras?

5. ¿Cuántas "palabras" de dos letras que terminen en consonante?

6. En cierto país las chapas de autos comprenden todas dos letras y tres cifras distintas de 0.
   ¿Cuántas chapas hay que empiezan con 3A y terminan con B?

2 – PRODUCTO DE VARIOS CONJUNTOS

He aquí los conjuntos A, B

Se saca un objeto de cada conjunto.

Este hecho puede representarse por la cupla (a, b)

El número de veces que eso se puede hacer, es el cardinal del conjunto de cuplas, es decir $\#(A \times B)$

En virtud de la definición de multiplicación de cardinales :

$$\#(A \times B) = \# A \cdot \# B$$

He aquí los conjuntos A, B, C

Se saca un objeto de cada conjunto y este hecho se anota (a, b, c) con $a \in A$, $b \in B$, $c \in C$

El conjunto de hechos consistentes en sacar un objeto de cada conjunto será designado mediante $A \times B \times C$

$$A \times B \times C = \{ (a, b, c) \mid a \in A, b \in B, c \in C \}$$

Es claro que

$$(a, b, c) = (a', b', c') \iff a = a' \quad \text{y} \quad b = b' \quad \text{y} \quad c = c'$$

Propongámonos calcular el número de veces que podemos sacar un objeto de cada conjunto, es decir

$$\#(A \times B \times C)$$

Observemos que

$$A \times B \times C \to (A \times B) \times C : (a, b, c) \to ((a, b), c)$$

es una biyección.

Luego

$$\begin{aligned} & \#(A \times B \times C) \\ = \ & \#((A \times B) \times C) && \text{en virtud de la biyección indicada.} \\ = \ & \#(A \times B) \cdot \#C && \text{definición de la multiplicación de cardinales.} \\ = \ & \#A \cdot B \cdot \#C && \text{definición y asociatividad de la multiplicación.} \end{aligned}$$

PROBLEMAS

1. ¿Cuántas "palabras" de tres letras que empiezan por vocal y terminan en consonante se pueden escribir?

(*Respuesta* : 3.120)

2. Define $A \times B \times C \times D$ y establece que
$\#(A \times B \times C \times D) = \#A \cdot \#B \cdot \#C \cdot \#D$

3. Generaliza el ejercicio anterior.

4. En cierto país las chapas de automóviles están compuestas de tres cifras y dos letras. Sabiendo que las letras O e I han sido excluidas, quieres decirnos cuántas chapas, en las cuales el segundo y el cuarto signo son letras, pueden distribuirse?

(*Respuesta* : 576.000)

$$A_1 \times A_2 \times \ldots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid a_1 \in A_1, \ldots, a_n \in A_n\}$$

$$(a_1, \ldots, a_n) = (b_1, \ldots, b_n) \iff a_1 = b_1, \ldots, a_n = b_n$$

$$\#(A_1 \times A_2 \times \ldots \times A_n) = \#A_1 \cdot \#A_2 \cdot \ldots \cdot \#A_n$$

3 – NUMERO DE APLICACIONES DEL CONJUNTO FINITO A EN EL CONJUNTO FINITO B

He aquí los conjuntos finitos A y B

Sea $a = \#A$, $b = \#B$

Calculemos el número de aplicaciones $A \to B$

Dibuja un esquema de $A \times B$ utilizando el mismo color para las flechas que parten de un mismo punto de A

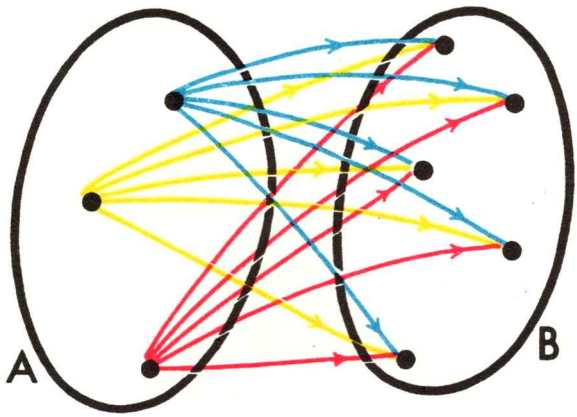


FIG. 1

– ¿Qué es una aplicación $A \to B$?

– Es un conjunto de flechas que parten de A y llegan a B
y tal que de todo punto de A parte una y sólo una flecha.

– ¿Cómo hacer para construir una aplicación $A \to B$?

– Se saca una flecha del ramillete azul, una del ramillete amarillo y una del rojo.

– El número de aplicaciones $A \to B$ es por lo tanto igual al número de veces que hagamos eso.

Calcular el número de aplicaciones $A \to B$ consiste en calcular el número de veces que se puede tomar una y sólo una flecha de cada uno de los ramilletes de color.

– ¿Cuántos de estos ramilletes hay?

– Hay a ramilletes.

– ¿Cuál es el cardinal de cada ramillete?

– El cardinal de cada ramillete es b.

– ¿Cuántas veces se puede tomar una y sólo una flecha de cada ramillete?

El número de veces que podemos hacer eso es

$$\underbrace{b \cdot b \cdot \ldots \cdot b}_{\text{a factores}} = b^a$$

TEOREMA 1

SI **los conjuntos finitos A y B comprenden a y b elementos respectivamente,**

ENTONCES **el número de aplicaciones $A \to B$ es b^a**

El conjunto de aplicaciones $A \to B$ se designa mediante B^A

Si A y B son finitos

Entonces el teorema 1 se expresa mediante la fórmula

$$\#(B^A) = (\#B)^{\#A}$$

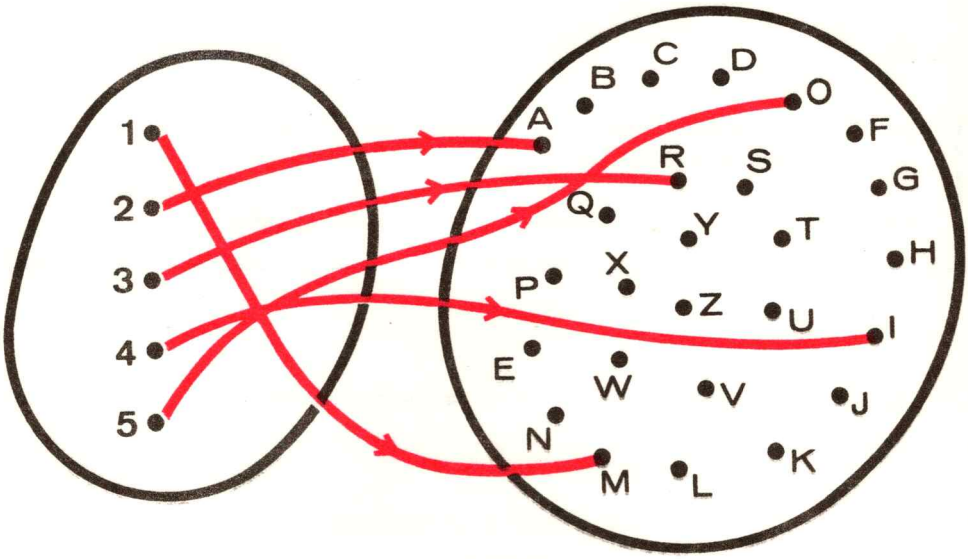
EJERCICIOS

1. ¿Cuál es el número de aplicaciones $\{ 1, 2, 3 \} \rightarrow \{ 0, 5, 6, 7 \}$?

2. ¿Cuál es el número de aplicaciones $\{ 0, 5, 6, 7 \} \rightarrow \{ 1, 2, 3 \}$?

3. Dibuja un conjunto A de cardinal 3 y un conjunto B de cardinal 1
   Dibuja las aplicaciones $A \rightarrow B$ y las aplicaciones $B \rightarrow A$
   ¿Cuántas son las aplicaciones $A \rightarrow B$ y cuántas las aplicaciones $B \rightarrow A$?

4. Toda "palabra" de cinco letras define una aplicación
   $$\{ 1, 2, 3, 4, 5 \} \rightarrow \{ a, b, c, \ldots, y, z \}$$
   He aquí el esquema de la función definida por **Mario**

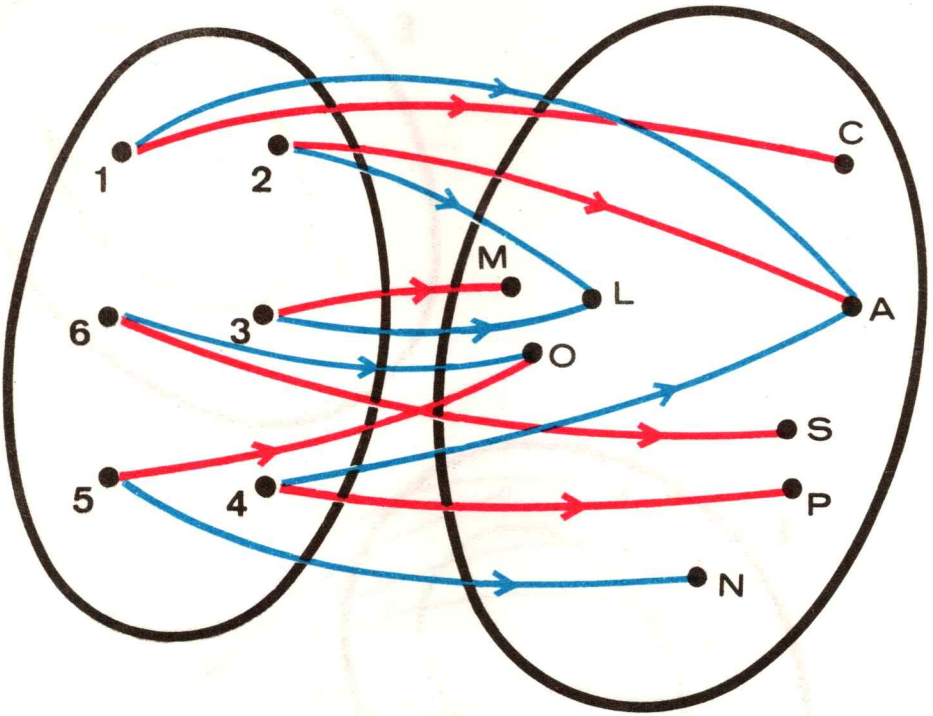


MARIO

FIG. 2

5. ¿Cuántas "palabras" de seis letras podemos formar?

6. Descifra el mensaje que acaba de recibir el jefe de Estado de un país en guerra.



MENSAJE AL JEFE DE ESTADO

FIG. 3

7. En cierto país las chapas de automóviles comprenden 5 signos que pueden ser cifras o letras distintas de O e I

¿Cuántos automóviles pueden tener tales chapas?

4 – NUMERO DE PARTES DE UN CONJUNTO

He aquí un conjunto E
y una de sus partes P

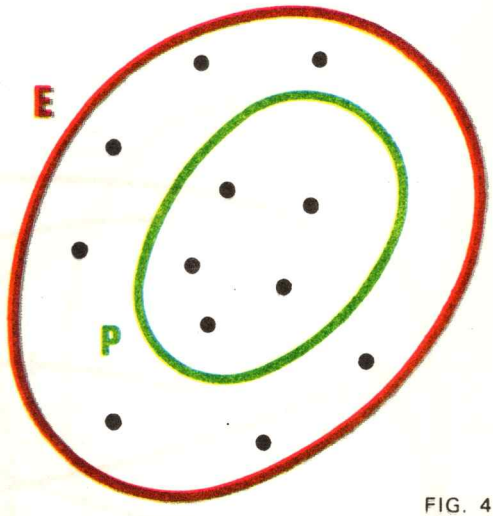


FIG. 4

Esta parte P define
la función

$p : E \rightarrow \{0, 1\}$

llamada **función característica de la parte P de E**

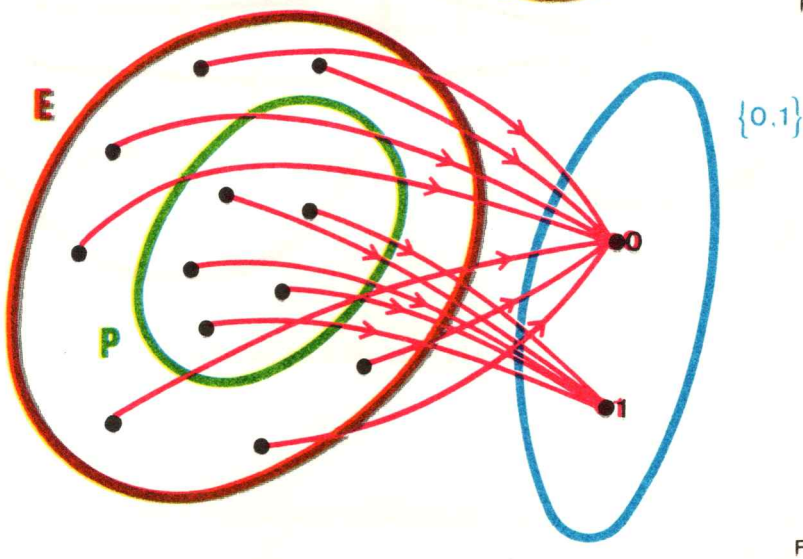


FIG. 5

$$p : E \rightarrow \{0, 1\}$$

FUNCION CARACTERISTICA DE LA PARTE P DE E

La función característica de la parte P de E está definida de la manera siguiente:

Para todo $x \in P$: $p(x) = 1$

Para todo $x \in E \setminus P$: $p(x) = 0$

El nombre de *función característica* de la parte P de E es muy adecuado :

dado p podemos hallar P

En efecto,

$$P = p^{-1}\{1\} = \{x \in E \mid p(x) = 1\}$$

Toda aplicación f: $E \to \{0, 1\}$ es **característica** de la parte $F = f^{-1}\{1\}$ de E

Así,

$\mathcal{P}E \to \{0,1\}^E$: $P \to p$ es una biyección

del conjunto $\mathcal{P}E$ de las partes de E

sobre

el conjunto $\{0, 1\}^E$ de aplicaciones $E \to \{0, 1\}$

Luego, el número de partes de un conjunto finito E que comprende n objetos es igual al número de funciones $E \to \{0, 1\}$,

es decir, es 2^n (en virtud del Teorema 1)

TEOREMA 2

Todo conjunto finito de n elementos contiene 2^n partes.

Para todo conjunto finito E

$$\#\mathcal{P}E = 2^{\#E}$$

EJERCICIOS

1. ¿Cuál es la función característica de la parte E de E?

2. ¿Cuál es la función característica de la parte vacía de E?

3. **Si** f designa la función característica de la parte F del conjunto E
   Entonces cuál es la parte de E que admite como característica la función g definida por

$$\text{para todo } x \in E \quad : \quad g(x) = 1 - f(x)$$

4. **Si** a y b designan las funciones características de dos partes disjuntas A y B de E
   Entonces cuál es la parte F de E cuya función característica f está definida por

$$\text{para todo } x \in E \quad : \quad f(x) = a(x) + b(x)$$

5. **Si** f y g designan las funciones características de las partes F y G de E
   Entonces cuál es la función característica de la parte $F \cap G$

6. Calcula $\# \mathcal{P}\{1, 2, 3, 4, 5\}$, $\# \mathcal{P}\{1\}$, $\# \mathcal{P}\{o\}$, $\# \mathcal{P}\phi$, $\# \mathcal{P}\{3, 3 + 4, 7\}$

5 – NUMERO DE INYECCIONES DEL CONJUNTO FINITO A EN EL CONJUNTO FINITO B

– He aquí los conjuntos finitos A y B que comprenden a y b elementos respectivamente

¿A qué se llama inyección de A en B?

– Se llama inyección de A en B a toda aplicación $f : A \to B$ tal que
para todo $x, y \in A$: $x \neq y \implies f(x) \neq f(y)$

– Vayamos a la figura 1, p. 6.

Para calcular el número de aplicaciones A → B observamos que se obtenía cada función tomando una sola flecha de cada ramillete que partía de A.

Ahora no podremos proceder tan libremente. Una vez que hayamos elegido una flecha azul, ya no podremos tomar una de las flechas amarillas, una de las rojas, ... (puesto que dos flechas distintas de una inyección no pueden llegar al mismo punto).

De modo que para toda elección de una flecha azul, tenemos posibilidades de tomar una amarilla de un ramillete de $b - 1$ flechas.

La elección de la flecha amarilla prohibe la elección de una nueva flecha roja, ...

Para toda elección de una flecha azul y de una amarilla, podremos sacar una flecha roja de un ramillete que tendrá $b - 2$ flechas, etc.

El número de inyecciones A → B es por lo tanto igual al número de maneras en que podemos sacar simultáneamente una flecha azul de un ramillete de b flechas, una flecha amarilla de un ramillete de $b - 1$ flechas, una flecha roja de un ramillete de $b - 2$ flechas, etc.

En virtud del § 2, sabemos que este número es

$$\underbrace{b \cdot (b-1) \cdot (b-2) \cdot \ldots \cdot (b-a+1)}_{\text{a factores}}$$

TEOREMA 3

El número de inyecciones de un conjunto finito A que comprende a elementos en un conjunto finito B que comprende b elementos es igual a

$$\underbrace{b \cdot (b-1) \cdot (b-2) \cdot \ldots \cdot (b-a+1)}_{\text{a factores}}$$

EJERCICIOS

1. Vimos que toda palabra de 6 letras define una función

$$\{1, 2, 3, 4, 5, 6\} \rightarrow \{a, b, c, d, \ldots, x, y, z\}$$

¿Entre las palabras siguientes, cuáles definen una inyección? :
¿sumiso, laucha, amigos, cabina, celada, Celina, acción, cuerpo, cadena, suelos, católicos, socialista?

2. Calcula el número de "palabras" formadas por 5 letras distintas.

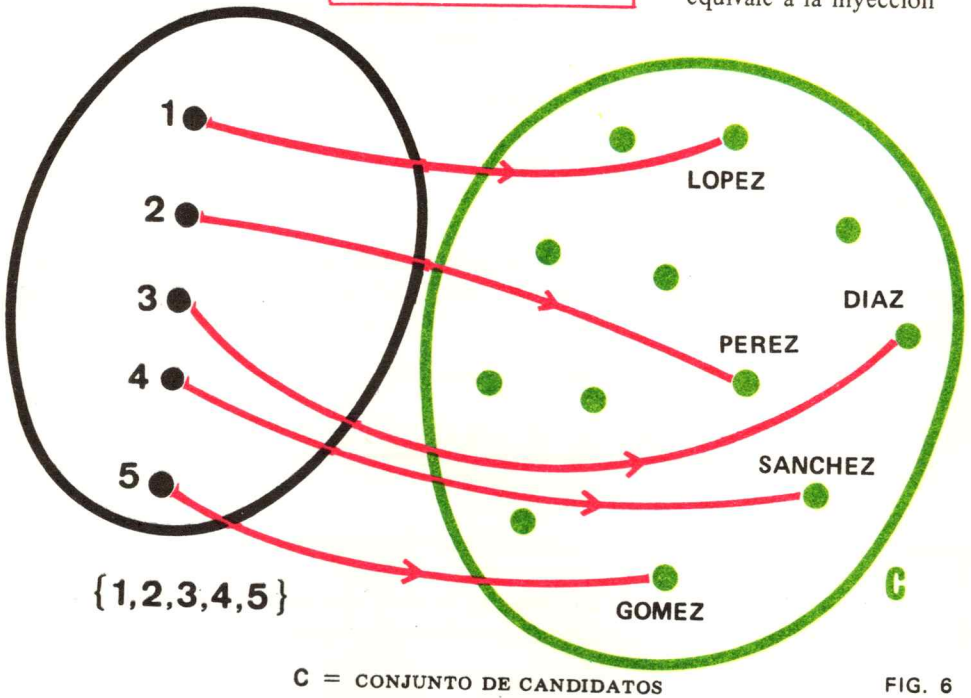
¿Cuántas de esas palabras terminan en *d*?

3. Esta asamblea de 450 personas debe elegir un comité de 5 miembros entre 12 candidatos. Cada uno de los 450 participantes debe votar por 5 candidatos distintos, indicando el orden de preferencias.

Esta boleta de elección

1. López
2. Pérez
3. Díaz
4. Sánchez
5. Gómez

equivale a la inyección



C = CONJUNTO DE CANDIDATOS

FIG. 6

De cuántas maneras posibles cada participante puede llenar una boleta válida de elección?

(*Respuesta* : 95.040)

4. ¿Cuántas "palabras" de 7 letras distintas que empiecen por *a* y terminen en *s* se pueden formar?

5. Calcula el número de "palabras" de 7 letras distintas que empiezan con consonante y terminan en vocal.

(*Respuesta* : 612.057.600)

6. Deseamos recompensar a 4 niños dando a cada uno un juguete elegido entre 10 juguetes muy distintos uno del otro. ¿De cuántas maneras puede efectuarse esta recompensa?

7. He aquí los conjuntos finitos A y B que comprenden *a* y *b* elementos respectivamente.

Si $b < a$

Entonces ¿cuál es el número de inyecciones A → B?

Sabemos que en este caso no existen inyecciones A → B

Por lo tanto el número de inyecciones A → B es 0

Observa que la fórmula del teorema 3 nos da este resultado.

8.

GRAN CONCURSO

Las palabras de once letras

MURCIELAGOS TIRABUZONES

definen cada una una *inyección* de ω {1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11} en el alfabeto.

Pedimos hallar las palabras más largas de la lengua española que definan una inyección.

Los ganadores recibirán como recompensa un turrón abstracto.

6 – BIYECCIONES Y PERMUTACIONES

He aquí los conjuntos finitos A y B de igual cardinal n

Toda biyección $A \to B$ es evidentemente una inyección $A \to B$

He aquí una inyección f: $A \to B$

Ella define la biyección f: $A \to fA$

Luego $\# fA = n = \# B$

de dónde $B = fA$ y f es una biyección $A \to B$

Si **A** *y* **B** *son conjuntos finitos equipotentes*

Entonces **f** *es una inyección* **A** $\to$ **B** **ssi** **f** *es una biyección* **A** $\to$ **B**

El número de biyecciones $A \to B$ es igual al número de inyecciones $A \to B$ es decir, (de acuerdo con la fórmula del teorema 3) :

$$\underbrace{n \cdot (n-1) \cdot \ldots \cdot 2 \cdot 1}_{n \text{ factores}}$$

Se llama **permutación de A**, a toda biyección $A \to A$

Y además el número de permutaciones de A es $\underbrace{n \cdot (n-1) \cdot \ldots \cdot 2 \cdot 1}_{n \text{ factores}}$

El número de permutaciones de un conjunto depende únicamente del número de elementos de dicho conjunto.

DEFINICION – **Para todo** $\mathfrak{n} \in \omega$, **se llama factorial de** $\mathfrak{n}$, **y se anota** $\mathfrak{n}!$ **al número de permutaciones de todo conjunto que comprende** $\mathfrak{n}$ **elementos.**

TEOREMA 4

SI A y B son conjuntos finitos de igual cardinal n.

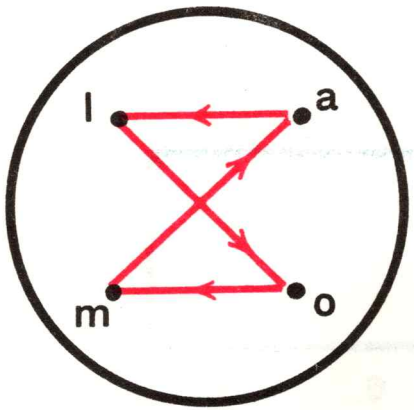
ENTONCES el número de biyecciones $A \to B$ es igual al número de permutaciones de A es decir $n! = \underbrace{n \cdot (n-1) \cdot \ldots \cdot 2 \cdot 1}_{n \text{ factores}}$

Observación : La permutación vacía es la única permutación del conjunto vacío.

De donde resulta la fórmula $0! = 1$

EJERCICIOS

1. Calcula el número de permutaciones de los conjuntos de cardinal 1, 2, 3, . . . , 9, 10
2. Para todo natural no nulo n :
$$2^{n-1} \leqslant n\,! \leqslant n^n$$
3. $\# \mathfrak{S} \{ 1, 2, 3, 4, 5, 6 \} = 720$
4. Calcula $\# \mathfrak{S} \{ 3.319.347 \}$
5. Todo anagrama de la palabra "malo" define una permutación de $\{ m, a, l, o \}$ Así por ejemplo, el anagrama "loma" define la permutación



PERMUTACION DEFINIDA POR EL ANAGRAMA LOMA DE MALO

FIG. 7

Toda permutación de $\{m, a, l, o\}$ proporciona un anagrama (con sentido o no) de la palabra "malo"

Calcula el número de anagramas de la palabra **"malo"** (considerando malo como uno de sus anagramas).

6. Dibuja el esquema definido por el anagrama **"zorba"** de **"brazo"**.
¿Cuántos anagramas posee la palabra **"brazo"**?

7. **Si** n y p son números naturales tales que $0 \leqslant p \leqslant n$

Entonces $$\frac{n!}{p!} = n \cdot (n-1) \cdot \ldots \cdot (p+1)$$

$$\frac{n!}{(n-p)!} = \underbrace{n \cdot (n-1) \cdot \ldots \cdot (n-p+1)}_{p \text{ factores}}$$

8.

TEOREMA 3

El número de inyecciones de un conjunto de p objetos en un conjunto de n objetos es $\dfrac{n!}{(n-p)!}$

9. El ama de casa aún no dispuso de qué manera sus invitados se ubicarán para cenar. Antes que lo haga, asignemos un número a cada lugar.

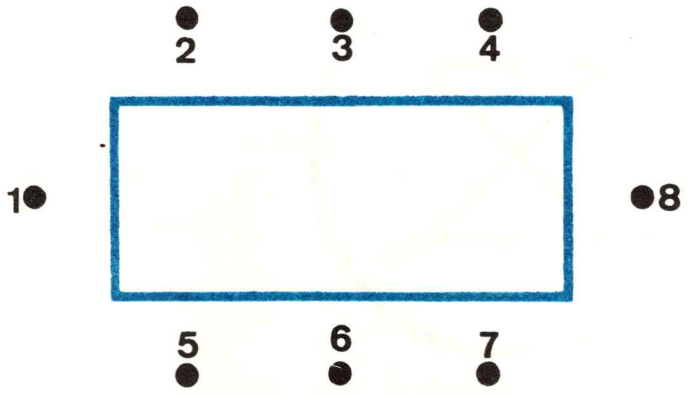


FIG. 8

El término $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 8 & 5 & 4 & 7 & 1 & 3 & 6 \end{pmatrix}$ define la permutación cuyo esquema es el siguiente

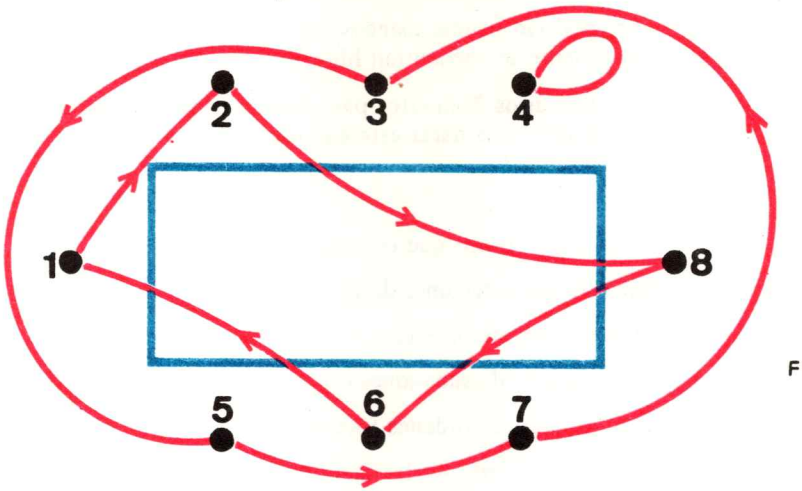


FIG. 9

Esta permutación (o su esquema) puede interpretarse como un "orden de mutación" de los convidados alrededor de la mesa.

Previamente el ama de casa había hecho la siguiente distribución :

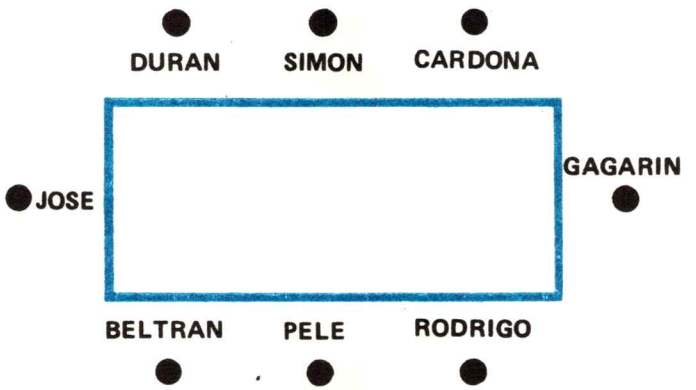


FIG. 10

Después de haber pensado mucho, decidió aplicar la permutación definida más arriba.

¿Cómo deberán ubicarse los invitados después de esta permutación?

¿Cómo se ubicarán después de haber aplicado la misma permutación dos veces seguidas?

¿De cuántas maneras distintas el ama de casa puede ubicar a sus invitados?

10. Los pupitres de tu clase están ubicados actualmente de una manera bien determinada.

¿De cuántas maneras podrían ocupar ustedes dichos pupitres, dejando desocupados los mismos que actualmente se encuentran libres?

Admitiendo que son necesarios 2 minutos para realizar cada disposición y que ustedes destinan 8 horas diarias para hacer este ejercicio ¿en qué fecha habrán tomado todas las ubicaciones posibles?

11. **Si** A es un conjunto finito que comprende n elementos,

Entonces el número de permutaciones de A

es igual al número de biyecciones $\{ 1, \ldots, n \} \rightarrow$ A

es igual al número de sucesiones $(a_1, \ldots, a_n)$ de elementos distintos de A

es igual al número de órdenes totales sobre A

es igual a $n! = 1 \cdot 2 \cdot \ldots \cdot (n-1) \cdot n$

7 – NUMERO DE PARTES DE p ELEMENTOS DE UN CONJUNTO FINITO DE n ELEMENTOS

He aquí un conjunto E que tiene 7 objetos.

Nos proponemos calcular el número de partes de E que tienen 3 elementos. Designaremos este número mediante el símbolo $\binom{7}{3}$

Toda parte P de 3 elementos de E se obtiene tomando un primer elemento de E, luego un segundo y finalmente un tercer elemento, es decir, definiendo una inyección $i : \{1, 2, 3\} \rightarrow E$

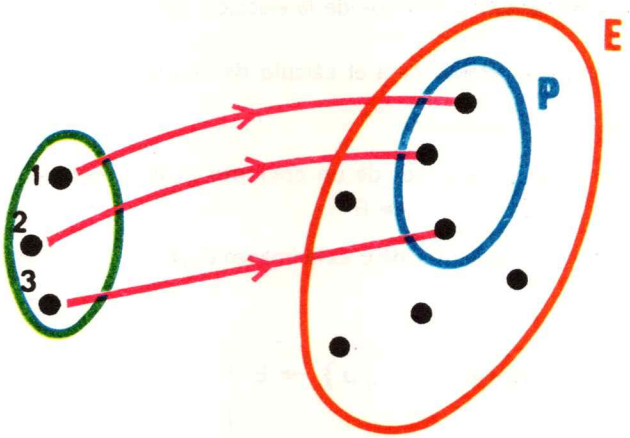


FIG. 11 $i: \{1,2,3\} \rightarrow E$

La imagen de toda inyección $\{1, 2, 3\} \rightarrow E$ es una parte de E que comprende 3 objetos.

He aquí una parte P de E que comprende 3 objetos.

– ¿Cuántas inyecciones $\{1, 2, 3\} \rightarrow E$ tienen como imagen P?

– Es el número de biyecciones $\{1, 2, 3\} \rightarrow P$ es decir, es 3!

– Hemos anotado $\binom{7}{3}$ el número de partes de E que tienen 3 objetos.

Por lo tanto el número de inyecciones $\{1, 2, 3,\} \rightarrow E$ será

$$\binom{7}{3} \times 3!$$

— Por el teorema 3 sabemos que el número de inyecciones $\{1, 2, 3\} \to E$ es

$$\frac{7!}{(7-3)!}$$

— Luego $$\binom{7}{3} \times 3! = \frac{7!}{(7-3)!}$$

$$\binom{7}{3} = \frac{7!}{3!\ (7-3)!} = 35$$

Este razonamiento no depende de la elección particular de los números 7 y 3.

Resumiremos las etapas para el cálculo del número $\binom{n}{p}$ de partes de p elementos de un conjunto de n elementos.

Toda parte de p elementos de un conjunto E de n elementos es la imagen de una inyección $\{1, 2, \ldots, p\} \to E$

Cada parte de p elementos de E es la imagen de $p!$ inyecciones $\{1, 2, \ldots, p\} \to E$ distintas.

El número de inyecciones $\{1, \ldots, p\} \to E$ es por lo tanto igual al número de partes de p elementos de E multiplicado por el número de inyecciones que tienen la misma imagen De donde resulta el

$$\frac{n!}{(n-p)} = \underbrace{n\,(n-1)\ldots(n-p+1)}_{p \text{ factores}}$$

$$\binom{n}{p}$$

$$p! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot p$$

TEOREMA 5

En un conjunto de n elementos, el número de partes de p elementos es igual a

$$\binom{n}{p} = \frac{n \cdot (n-1) \cdot \ldots \cdot (n-p+1)}{1 \cdot 2 \cdot \ldots \cdot p} = \frac{n!}{(n-p)!\ p!}$$

EJERCICIOS

1. He aquí un conjunto de 4 elementos, $E = \{a, b, c, d\}$

Enumera todas las partes de E que comprenden 0, 1, 2, 3, 4, elementos.

Cuéntalas y verifica que tienes los números indicados por la fórmula recuadrada p. 22.

Existen tantas partes de 0 elementos como partes de 4 elementos, y tantas partes de 1 elemento como partes de 3 elementos. ¿Por qué? ¿Esto no te sugiere una fórmula?

La suma de los números que hallaste para las partes de 0, 1, 2, 3, 4, elementos es 2^4. ¿Por qué?

¿Podrías generalizar dando una fórmula interesante?

2. ¿Cuántas partes de 7 elementos hay en un conjunto de 15 elementos?

3. ¿De cuántas maneras se puede formar una delegación de 3 alumnos en un curso de 28 alumnos?

4. He aquí 4 puntos distintos tales que ninguna recta comprende tres de ellos.

¿Cuántas rectas que comprenden dos de estos puntos existen?

5. En esta escuela se inscribieron 57 alumnos en el mismo curso. ¿De cuántas maneras se puede realizar un desdoblamiento en una clase de 28 y otras de 29 alumnos?

6. ¿De cuántas maneras se pueden repartir 56 alumnos inscriptos para los mismos estudios en dos cursos de 28 alumnos, uno dirigido por la señorita Violeta y el otro por la señorita Hortensia?

7. ¿Por qué en el ejercicio 6 indicamos el nombre de las profesoras de cada clase, contrariamente a lo que hicimos en el ejercicio 5?

8. En tal país hay 300 diputados y 200 senadores. ¿De cuántas maneras se puede formar una comisión mixta compuesta de 3 diputados y 2 senadores?

9. Utilizando la fórmula del teorema 5, calcula el número de conjuntos unitarios, el número de pares y el número de partes de $(n - 1)$ elementos que contiene un conjunto de n elementos.

10. El número de pares contenidos en un conjunto de **n** elementos es $\frac{n \cdot (n - 1)}{2}$

8 – PROPIEDADES DE $\binom{n}{p}$

a) El conjunto vacío no contiene más que la parte vacía.

Luego $$\binom{0}{0} = 1$$

b) Todo conjunto sólo contiene una parte que contiene 0 elemento.

Luego, para todo $n \in \omega$:

$$\binom{n}{0} = 1$$

c) Todo conjunto finito de n elementos contiene una única parte de n elementos.

Luego, para todo $n \in \omega$:

$$\binom{n}{n} = 1$$

d) Ningún conjunto finito de n elementos contiene alguna parte que comprenda más de n elementos.

Luego

$$p > n \implies \binom{n}{p} = 0$$

e) Todo conjunto finito de n elementos contiene n conjuntos unitarios.

De donde, para todo $n \in \omega$:

$$\binom{n}{1} = n$$

f) He aquí un conjunto E que comprende n elementos.

Si para todo $p \in \omega$ tal que $0 \leqslant p \leqslant n$

$\mathscr{P}_p$ E es el conjunto de partes de E que comprende p elementos,

Entonces $\mathscr{P}_p$ E $\rightarrow$ $\mathscr{P}_{n-p}$ E : P $\rightarrow$ E $\setminus$ P es una biyección.

TEOREMA 6

En un conjunto de n elementos, el número de partes de cardinal p es igual al número de partes de cardinal (n − p)

$$\binom{n}{p} = \frac{n!}{p!\ (n-p)!} = \binom{n}{n-p}$$

g) En un conjunto de n elementos, los números de partes que comprenden :

$$0 \quad , \quad 1 \quad , \quad 2 \quad , \ \ldots \ , \quad n-1 \quad , \quad n$$

elementos son respectivamente

$$\binom{n}{0} \ , \ \binom{n}{1} \ , \ \binom{n}{2} \ , \ \ldots \ , \ \binom{n}{n-1} \qquad \binom{n}{n}$$

Pero sabemos que el número total de partes de tal conjunto es 2^n

De donde resulta la fórmula

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{n-1} + \binom{n}{n} = 2^n$$

9 – TRIANGULO DE PASCAL

n \ p	0	1	2	3	4	5	6	7		p	
0	$\binom{0}{0}$	$\binom{0}{1}$	$\binom{0}{2}$	$\binom{0}{3}$	$\binom{0}{4}$	$\binom{0}{5}$	$\binom{0}{6}$	$\binom{0}{7}$		$\binom{0}{p}$	
1	$\binom{1}{0}$	$\binom{1}{1}$	$\binom{1}{2}$	$\binom{1}{3}$	$\binom{1}{4}$	$\binom{1}{5}$	$\binom{1}{6}$	$\binom{1}{7}$		$\binom{1}{p}$	
2	$\binom{2}{0}$	$\binom{2}{1}$	$\binom{2}{2}$	$\binom{2}{3}$	$\binom{2}{4}$	$\binom{2}{5}$	$\binom{2}{6}$	$\binom{2}{7}$		$\binom{2}{p}$	
3	$\binom{3}{0}$	$\binom{3}{1}$	$\binom{3}{2}$	$\binom{3}{3}$	$\binom{3}{4}$	$\binom{3}{5}$	$\binom{3}{6}$	$\binom{3}{7}$		$\binom{3}{p}$	
4	$\binom{4}{0}$	$\binom{4}{1}$	$\binom{4}{2}$	$\binom{4}{3}$	$\binom{4}{4}$	$\binom{4}{5}$	$\binom{4}{6}$	$\binom{4}{7}$		$\binom{4}{p}$	
5	$\binom{5}{0}$	$\binom{5}{1}$	$\binom{5}{2}$	$\binom{5}{3}$	$\binom{5}{4}$	$\binom{5}{5}$	$\binom{5}{6}$	$\binom{5}{7}$		$\binom{5}{p}$	
6	$\binom{6}{0}$	$\binom{6}{1}$	$\binom{6}{2}$	$\binom{6}{3}$	$\binom{6}{4}$	$\binom{6}{5}$	$\binom{6}{6}$	$\binom{6}{7}$		$\binom{6}{p}$	
7	$\binom{7}{0}$	$\binom{7}{1}$	$\binom{7}{2}$	$\binom{7}{3}$	$\binom{7}{4}$	$\binom{7}{5}$	$\binom{7}{6}$	$\binom{7}{7}$		$\binom{7}{p}$	
n	$\binom{n}{0}$	$\binom{n}{1}$	$\binom{n}{2}$	$\binom{n}{3}$	$\binom{n}{4}$	$\binom{n}{5}$	$\binom{n}{6}$	$\binom{n}{7}$		$\binom{n}{p}$	

CUADRO DE LOS $\binom{n}{p}$ FIG. 12

Se trata de reemplazar cada uno de los símbolos $\binom{n}{p}$ por el número que designa. Empecemos por tener en cuenta que en virtud de la observación b del parágrafo 8, la primera columna del cuadro comprende solamente 1.

En virtud de la observación c del mismo parágrafo,

$$\binom{0}{0} = \binom{1}{1} = \binom{2}{2} = \ldots = \binom{n}{n} = \ldots = 1$$

De modo que la diagonal del cuadro también está compuesta de 1

En virtud de la observación d del parágrafo 8, todas las casillas situadas a la derecha de esta diagonal deben comprender cero.

Llevemos estos resultados al cuadro.

n \ p	0	1	2	3	4	5	6	7	8	9	10	11	12
0	1	0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	0	0	0	0	0	0	0	0	0	0	0
2	1		1	0	0	0	0	0	0	0	0	0	0
3	1			1	0	0	0	0	0	0	0	0	0
4	1				1	0	0	0	0	0	0	0	0
5	1					1	0	0	0	0	0	0	0
6	1						1	0	0	0	0	0	0
7	1							1	0	0	0	0	0
8	1								1	0	0	0	0
9	1									1	0	0	0
10	1										1	0	0
11	1											1	0

CUADRO DE LOS $\binom{n}{p}$ FIG. 13

Para llenar las otras casillas de este cuadro, podrías utilizar la fórmula del teorema 5.

Procederemos de una manera más expeditiva utilizando una fórmula debida a **Pascal.**

Veremos que cada vez que en el cuadro se consideran tres casillas dispuestas de esta manera

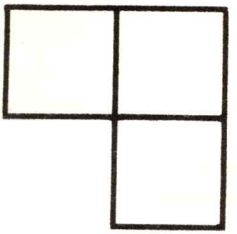


FIG. 14

el número que figura en la casilla de abajo es la suma de los números de las casillas de arriba.

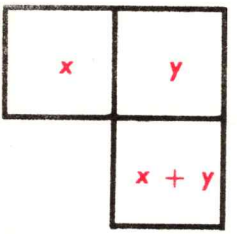
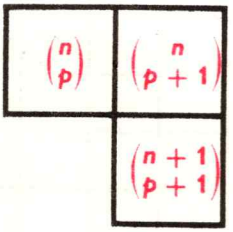


FIG. 15

Ahora será suficiente que pasees esta pequeña escuadra por el cuadro, para completarlo mediante simples adiciones.

TEOREMA 7



$$\binom{n+1}{p+1} = \binom{n}{p} + \binom{n}{p+1}$$

FORMULA DE PASCAL

FIG. 16

DEMOSTRACION :

He aquí un conjunto E que tiene $(n + 1)$ elementos.

Designemos con $\mathcal{P}$ el conjunto de partes de E que comprenden $(p + 1)$ elementos.

He aquí un elemento a de E

Llamemos $\mathcal{P}'$ al conjunto de elementos de $\mathcal{P}$ que comprenden a a y $\mathcal{P}''$ al conjunto de elementos de $\mathcal{P}$ que no comprenden a a

Claramente

$$\#\mathcal{P} = \#\mathcal{P}' + \#\mathcal{P}''$$

1° $$\#\mathcal{P} = \binom{n+1}{p+1}$$

2° $\mathcal{P}''$ es el conjunto de partes de $E \setminus \{a\}$ que comprenden $(p + 1)$ elementos.

Luego

$$\#\mathcal{P}'' = \binom{n}{p+1}$$

3° **Si** X recorre $\mathcal{P}'$

Entonces $X \setminus \{a\}$ recorre el conjunto de partes de $E \setminus \{a\}$ que comprenden p elementos.

De manera más precisa :

$\mathcal{P}' \rightarrow$ conjunto de partes de $E \setminus \{a\}$ que comprenden p elementos: $X \rightarrow X\{a\}$ es una biyección.

Luego

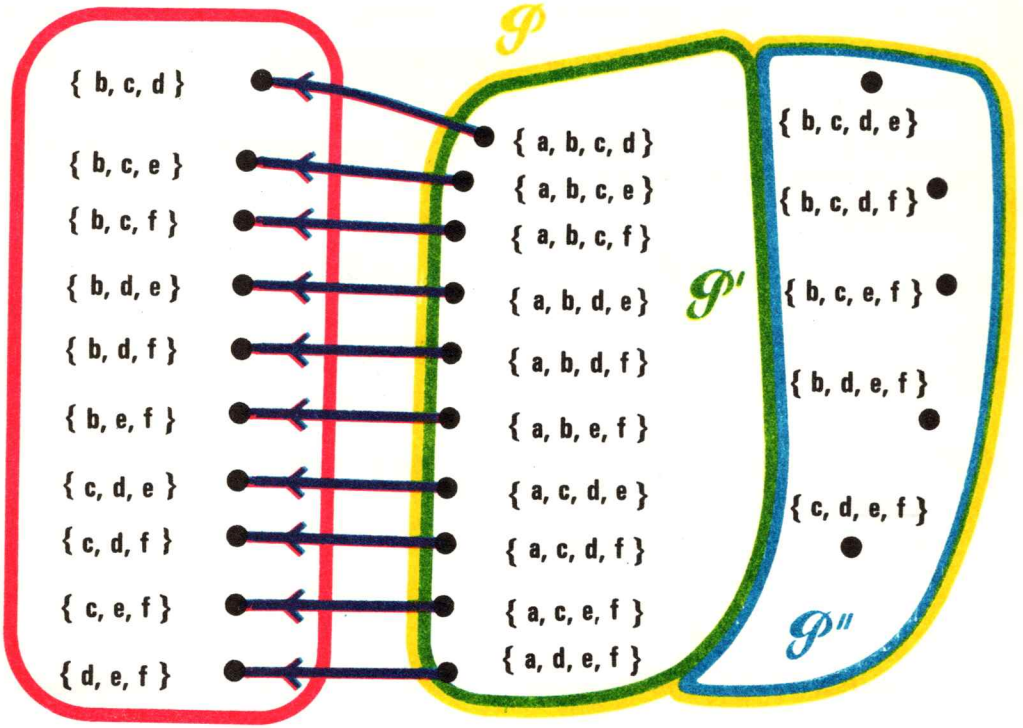
$$\#\mathcal{P}' = \binom{n}{p}$$

Finalmente, $\#\mathcal{P} = \#\mathcal{P}' + \#\mathcal{P}''$ implica

$$\boxed{\binom{n+1}{p+1} = \binom{n}{p+1} + \binom{n}{p}}$$

l. q. q. d.

ILUSTRACION DE LA DEMOSTRACION DE LA FORMULA DE PASCAL



$$\# = \# + \#$$

$$\# = \binom{6}{4}$$

$$\# = \# = \binom{5}{3}$$

$$\# = \binom{5}{4}$$

Luego

$$\boxed{\binom{6}{4} = \binom{5}{3} + \binom{5}{4}}$$

FIG. 17

Completemos el cuadro mediante este procedimiento.

n \ p	0	1	2	3	4	5	6	7	8	9	10	11	12
0	1	o	o	o	o	o	o	o	o	o	o	o	o
1	1	1	o	o	o	o	o	o	o	o	o	o	o
2	1	2	1	o	o	o	o	o	o	o	o	o	o
3	1	3	3	1	o	o	o	o	o	o	o	o	o
4	1	4	6	4	1	o	o	o	o	o	o	o	o
5	1	5	10	10	5	1	o	o	o	o	o	o	o
6	1	6	15	20	15	6	1	o	o	o	o	o	o
7	1	7	21	35	35	21	7	1	o	o	o	o	o
8	1	8	28	56	70	56	28	8	1	o	o	o	o
9	1	9	36	84	126	126	84	36	9	1	o	o	o
10	1	10	45	120	210	252	210	120	45	10	1	o	o
11	1	11	55	165	330	462	462	330	165	55	11	1	o
12	1	12	66	220	495	792	924	792	495	220	66	12	1

TRIANGULO DE PASCAL FIG. 18

EJERCICIOS

1. Convengamos en representar la fórmula del Pascal mediante el esquema

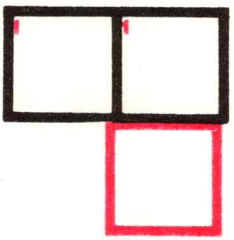


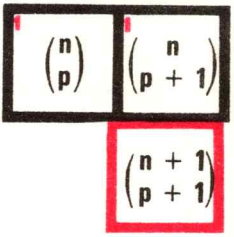
FIG. 19

que se interpreta de la manera siguiente :

El número del cuadro de Pascal situado en la casilla roja es igual a 1 vez el número situado en la primera casilla negra, más una vez el número situado en la última casilla negra.

Si pongo $\binom{n+1}{p+1}$ en la casilla roja.

¿Qué números habría que ubicar en las casillas negras?



En este esquema se lee claramente la fórmula de Pascal

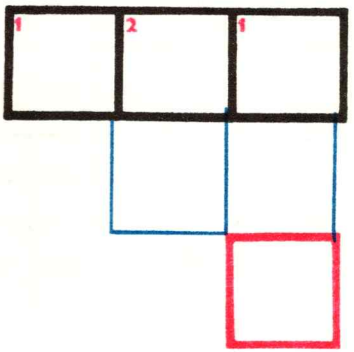
$$\binom{n+1}{p+1} = 1 \cdot \binom{n}{p} + 1 \cdot \binom{n}{p+1}$$

FIG. 20

Escribe las fórmulas que obtienes si ubicas en la casilla roja del primer esquema

$$\binom{n+1}{p+2} \quad , \quad \binom{n+2}{p+1} \qquad \binom{n+2}{p+2}$$

2. Explica y justifica el esquema siguiente



Qué fórmula se lee en este esquema cuando la casilla roja está ocupada por $\binom{n+2}{p+2}$

FIG. 21

3. ¿Quieres explicar y justificar este esquema?

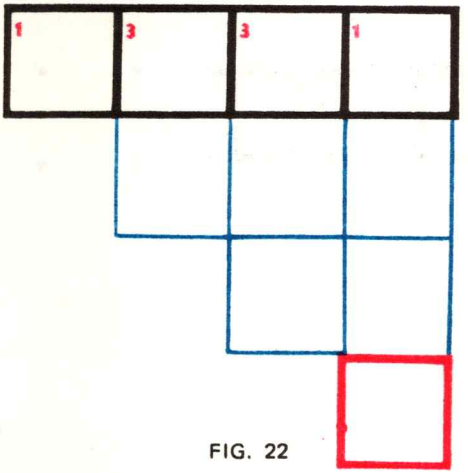


FIG. 22

¿Qué fórmulas se leen en el esquema cuando la casilla roja está ocupada por

$\binom{n+3}{p+3}$, $\binom{n+5}{p+6}$?

4. ¿Quieres explicar y justificar este esquema?

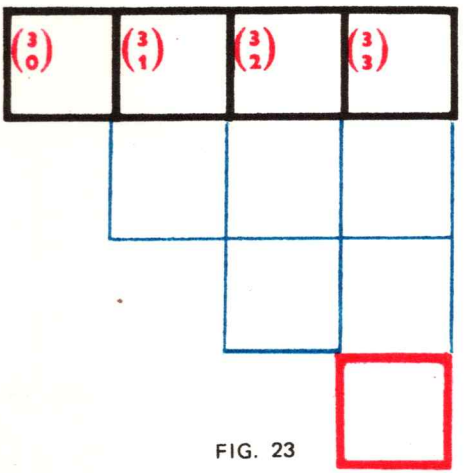


FIG. 23

Cuando la casilla roja está ocupada por $\binom{n+3}{p+3}$,

Se lee la fórmula siguiente

$$\binom{n+3}{p+3} = \binom{3}{0}\binom{n}{p} + \binom{3}{1}\binom{n}{p+1} + \binom{3}{2}\binom{n}{p+2} + \binom{3}{3}\binom{n}{p+3}$$

5. En los ejercicios anteriores comenzamos la construcción de un triángulo de Pascal apoyado sobre su punta.

Justifica las indicaciones del esquema siguiente.

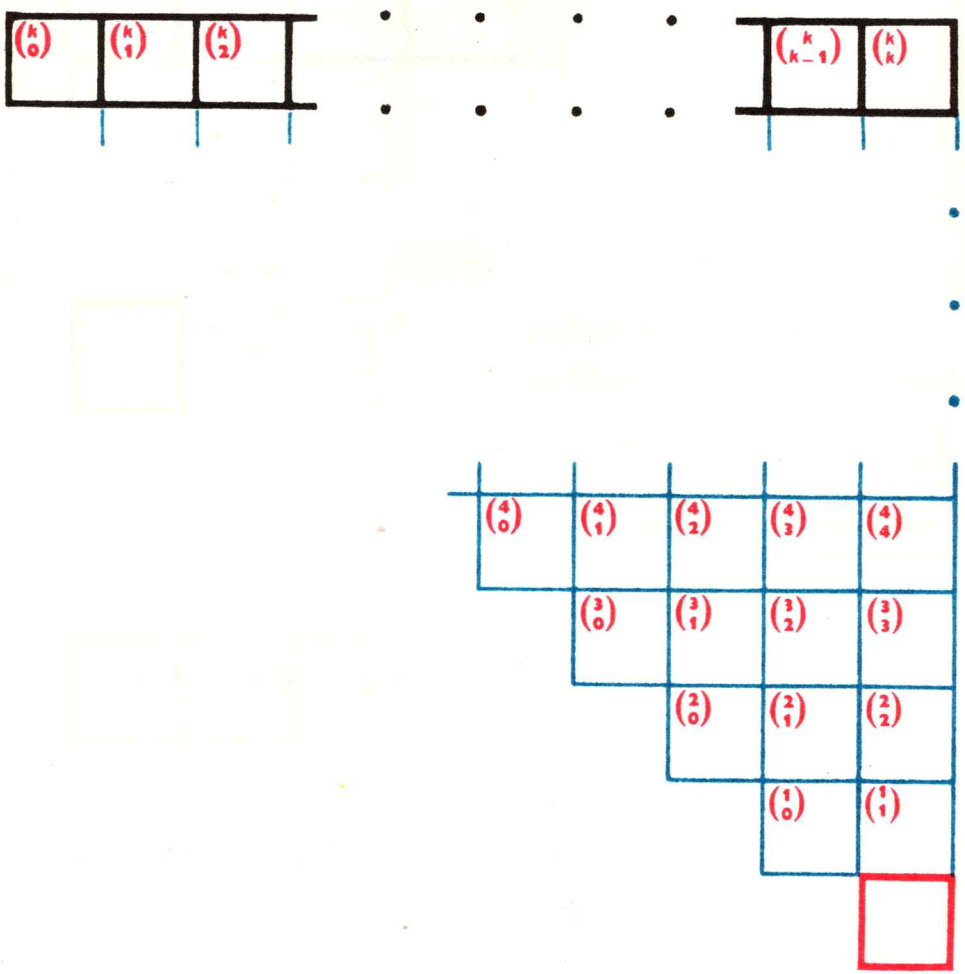
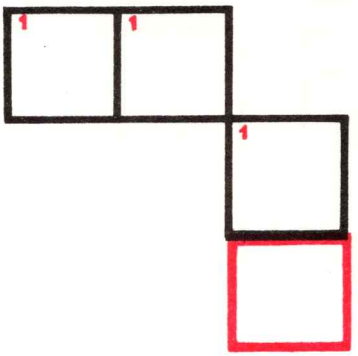


FIG. 24

Justifica la fórmula

$$\binom{n+k}{p+k} = \binom{k}{0}\binom{n}{p} + \binom{k}{1}\binom{n}{p+1} + \ldots + \binom{k}{k-1}\binom{n}{p+k-1} + \binom{k}{k}\binom{n}{p+k}$$

6. Los ejercicios anteriores ilustraron procedimientos que permiten descubrir numerosas fórmulas. ¿Quieres explicar y justificar los esquemas siguientes?



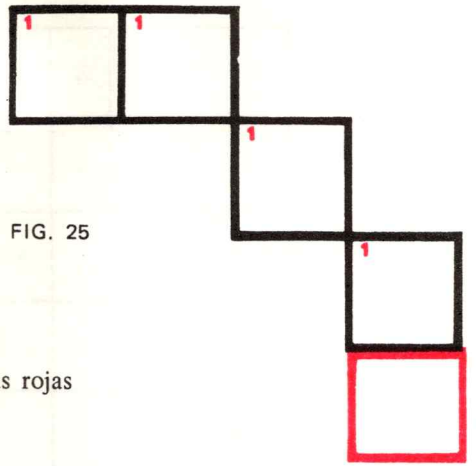


FIG. 25

¿Qué fórmulas se leen cuando las casillas rojas están ocupadas respectivamente

por $\binom{n+2}{p+2}$, $\binom{n+3}{p+3}$?

7. Explica y justifica el esquema

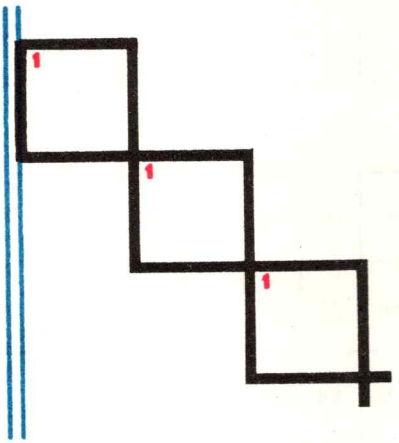
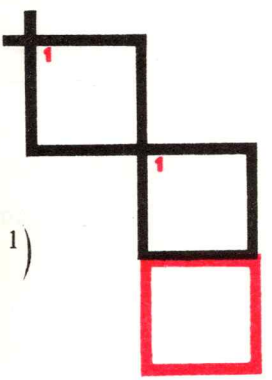


FIG. 26

Deduce la fórmula

$$\binom{n}{p} = \binom{n-1}{p} + \binom{n-2}{p-1} + \ldots$$

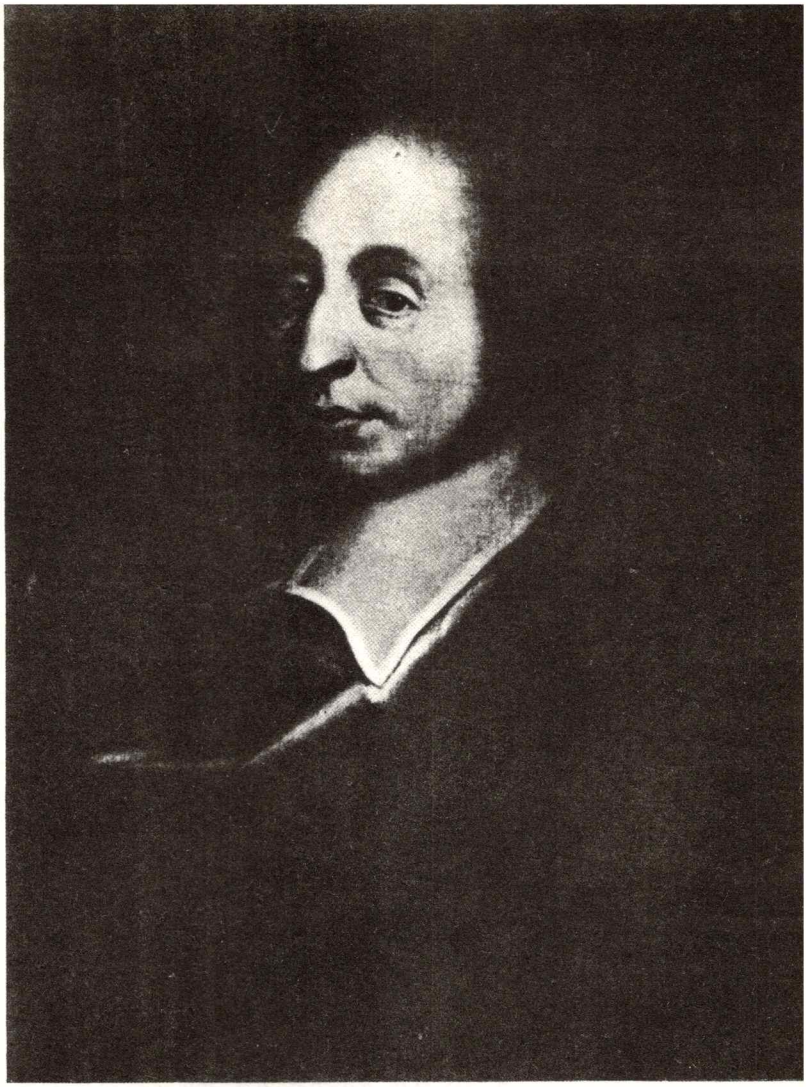
$$\binom{n-p+1}{2} + \binom{n-p}{1} + \binom{n-p-1}{0}$$



8. Los puntos rojos marcados en este cuadro están relacionados con la fórmula del teorema 6. ¡Explica y justifica!

p \ n	0	1	2	3	4	5	6	7	8	9	10	11	12
0	1	0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	0	0	0	0	0	0	0	0	0	0	0
2	1	2	1	0	0	0	0	0	0	0	0	0	0
3	1	3	3	1	0	0	0	0	0	0	0	0	0
4	1	4	6	4	1	0	0	0	0	0	0	0	0
5	1	5	10	10	5	1	0	0	0	0	0	0	0
6	1	6	15	20	15	6	1	0	0	0	0	0	0
7	1	7	21	35	35	21	7	1	0	0	0	0	0
8	1	8	28	56	70	56	28	8	1	0	0	0	0
9	1	9	36	84	126	126	84	36	9	1	0	0	0
10	1	10	45	120	210	252	210	120	45	10	1	0	0
11	1	11	55	165	330	462	462	330	165	55	11	1	0
12	1	12	66	220	495	792	924	792	495	220	66	12	1

FIG. 27



BLAS PASCAL (1623-1662)

Blas Pascal Nació en Clermont-Ferrand, donde su padre era un notable. Siguió a su familia en sus continuos desplazamientos por Francia; su salud fue precaria durante toda su vida.

A los 16 años ya había demostrado un importante teorema de geometría que lleva su nombre.

A los 18 inventó y construyó una máquina de calcular.

A los 23, Pascal, de familia católica, es conquistado por el Jansenismo, doctrina de tendencia rigorista.

A los 25 años observó el descenso de presión atmosférica experimentada al elevar un barómetro llevado al pico del Puyde-Dome.

A los 31 años, en su correspondencia con Fermat, funda la teoría de probabilidades, como consecuencia de una serie de preguntas formuladas por un jugador.

Poco después se retira definitivamente al convento Jansenista de Port-Royal.

A partir de 1656 publica sus famosas *Cartas Provinciales*, en las que pone en evidencia su talento de escritor al servicio de la polémica de los Jansenistas contra los jesuitas. Estas cartas, por otra parte, han contribuido grandemente a la fijación de la lengua francesa.

La obra en la cual utiliza el triángulo aritmético, llamado de Pascal, conocido ya anteriormente, se publicó después de su muerte en 1664.

10 – FORMULA DE NEWTON

a) Cada una de las letras *a, b, c, d, e,* designa un número real. Escribe todos los productos de tres **letras** distintas, tomadas de entre ellas, respetando el orden alfabético en cada uno de dichos **términos.**

a b c, a b d, a b e, a c d, a c e, a d e, b c d, b c e, b d e, c d e

¿Cómo podrías haber calculado la cantidad de tales términos?

– Este número de términos es igual al número de partes de 3 elementos incluidas en un conjunto de 5 elementos, es decir

$$\binom{5}{3} = \frac{5 \times 4 \times 3}{1 \times 2 \times 3} = 10$$

– Más generalmente, tendremos

$\binom{5}{1}$ productos de una sola letra :
a, b, c, d, e

$\binom{5}{2}$ productos de dos letras :
a b, a c, a d, a e, b c, b d, b e, c d, c e, d e

$\binom{5}{3}$ productos de tres letras :
a b c, a b d, a b e, a c d, a c e, a d e, b c d, b c e, b d e, c d e

$\binom{5}{4}$ productos de cuatro letras :
a b c d, a b c e, a b d e, a c d e, b c d e

$\binom{5}{5}$ producto de cinco letras :
a b c d e

b) *¡Calculemos!*

$$(x+a)(x+b)(x+c)(x+d)(x+e) = (x+a)^5$$

$$= x^5 + \underbrace{(a+b+c+d+e)}_{\binom{5}{1}\text{ términos}} x^4 = x^5 + \binom{5}{1} a\, x^4$$

$$+ \underbrace{(ab+ac+ad+ae+bc+bd+be+cd+ce+de)}_{\binom{5}{2}\text{ términos}} x^3 + \binom{5}{2} a^2\, x^3$$

$$+ \underbrace{(abc+abd+abe+acd+ace+ade+bcd+bce+bde+cde)}_{\binom{5}{3}\text{ términos}} x^2 + \binom{5}{3} a^3\, x^2$$

$$+ \underbrace{(abcd+abce+abde+acde+bcde)}_{\binom{5}{4}\text{ términos}} x + \binom{5}{4} a^4\, x$$

$$+ \underbrace{abcde}_{\binom{5}{5}\text{ términos}} + \binom{5}{5} a^5$$

Como $\binom{5}{0} = 1$, tenemos la bonita fórmula

$$(x+a)^5 = \binom{5}{0} x^5 + \binom{5}{1} a\, x^4 + \binom{5}{2} a^2\, x^3 + \binom{5}{3} a^3\, x^2 + \binom{5}{4} a^4\, x + \binom{5}{5} a^5$$

c) Cada una de las "letras" $a_1, a_2, \ldots, a_7$ designa un número.

Escribe todos los productos de cuatro letras distintas respetando el orden creciente de índices.

$a_1a_2a_3a_4$, $a_1a_2a_3a_5$, $a_1a_2a_3a_6$, $a_1a_2a_3a_7$, $a_1a_2a_4a_5$, . . . , $a_4a_5a_6a_7$

Cuenta el número de productos que obtuviste.

Veamos si no te equivocaste.

¿Cómo podríamos haber *calculado* el número de tales productos?

– Es el número de partes de cuatro elementos contenidas en un conjunto de 7 elementos, es decir

$$\binom{7}{4} = \frac{7 \times 6 \times 5 \times 4}{1 \times 2 \times 3 \times 4} = 35$$

– Generalizando, existen

$\binom{7}{1}$ = 7 productos de 1 letra : a_1 , a_2 , . . . , a_7

$\binom{7}{2}$ = 21 productos de 2 letras : $a_1\,a_2$, $a_1\,a_3$, . . . , $a_6\,a_7$

$\binom{7}{3}$ = 35 productos de 3 letras : $a_1a_2a_3$, $a_1a_2a_4$, . . . , $a_5a_6a_7$

$\binom{7}{4}$ = 35 productos de 4 letras : $a_1\,a_2\,a_3\,a_4$, . . . , $a_4\,a_5\,a_6\,a_7$

$\binom{7}{5}$ = 21 productos de 5 letras : $a_1\,a_2\,a_3\,a_4\,a_5$, . . . , $a_3\,a_4\,a_5\,a_6\,a_7$

$\binom{7}{6}$ = 7 productos de 6 letras : $a_1\,a_2\,a_3\,a_4\,a_5\,a_6$, . . . , $a_2\,a_3\,a_4\,a_5\,a_6\,a_7$

$\binom{7}{7}$ = 1 producto de 7 letras : $a_1\,a_2\,a_3\,a_4\,a_5\,a_6\,a_7$

d) ¡Calculemos!

$$(x+a_1)\cdot(x+a_2)\cdot(x+a_3)\cdot(x+a_4)\cdot(x+a_5)\cdot(x+a_6)\cdot(x+a_7) \qquad (x+a)^7$$

$$= x^7 \qquad = x^7$$

$$+ \underbrace{(a_1 + a_2 + \cdots + a_7)}_{\binom{7}{1}\text{ términos}}\, x^6 \qquad + \binom{7}{1} a\, x^6$$

$$+ \underbrace{(a_1\,a_2 + a_1\,a_3 + \ldots + a_6\,a_7)}_{\binom{7}{2}\text{ términos}}\, x^5 \qquad + \binom{7}{2} a^2\, x^5$$

$$+ \underbrace{(a_1\,a_2\,a_3 + a_1\,a_2\,a_4 + \ldots + a_5\,a_6\,a_7)}_{\binom{7}{3}\text{ términos}}\, x^4 \qquad + \binom{7}{3} a^3\, x^4$$

$$+ \underbrace{(a_1\,a_2\,a_3\,a_4 + a_1\,a_2\,a_3\,a_5 + \ldots + a_1\,a_5\,a_6\,a_7)}_{\binom{7}{4}\text{ términos}}\, x^3 \qquad + \binom{7}{4} a^4\, x^3$$

$$+ \underbrace{(a_1\,a_2\,a_3\,a_4\,a_5 + \ldots + a_3\,a_4\,a_5\,a_6\,a_7)}_{\binom{7}{5}\text{ términos}}\, x^3 \qquad + \binom{7}{5} a^5\, x^2$$

$$+ \underbrace{(a_1\,a_2\,a_3\,a_4\,a_5\,a_6 + \ldots + a_2\,a_3\,a_4\,a_5\,a_6\,a_7)}_{\binom{7}{6}\text{ términos}}\, x \qquad + \binom{7}{6} a^6\, x$$

$$+ \underbrace{a_1\,a_2\,a_3\,a_4\,a_5\,a_6\,a_7}_{\binom{7}{7}\text{ términos}} \qquad + \binom{7}{7} a^7$$

$$(x+a)^7 = \binom{7}{0}x^7 + \binom{7}{1}ax^6 + \binom{7}{2}a^2x^5 + \binom{7}{3}a^3x^4 + \binom{7}{4}a^4x^3 + \binom{7}{5}a^5x^2 + \binom{7}{6}a^6x + \binom{7}{7}a^7$$

e) El razonamiento anterior continúa siendo válido si reemplazamos el número 7 por cualquier natural.

De donde resulta **la fórmula de Newton**

$$(x+a)^n = \binom{n}{0}x^n + \binom{n}{1}a\,x^{n-1} + \ldots + \binom{n}{p}a^p\,x^{n-p} + \ldots + \binom{n}{n-1}a^{n-1}\,x + \binom{n}{n}a^n$$

EJERCICIOS

1. Utilizando la fórmula de Newton, vuelve a hallar las fórmulas

$$(x+a)^2 = x^2 + 2ax + a^2$$

$$(x+a)^3 = x^3 + 3a\,x^2 + 3a^2\,x + a^3$$

2. $$(x+a)^4 = x^4 + \binom{4}{1}a\,x^3 + \binom{4}{2}a^2\,x^2 + \binom{4}{3}a^3\,x + \binom{4}{4}a^4$$

$$= x^4 + \frac{4!}{1!\ 3!}a\,x^3 + \frac{4!}{2!\ 2!}a^2\,x^2 + \frac{4!}{3!\ 1!}a^3\,x + \frac{4!}{4!\ 1!}a^4$$

$$= x^4 + 4\,a\,x^3 + 6\,a^2\,x^2 + 4\,a^3\,x + a^4$$

Desarrolla igualmente $(x+a)^5$, $(x+a)^6$

3. Desarrollando $2^n = (1+1)^n$, halla nuevamente una fórmula ya conocida.

4. Desarrolla $(x-1)^2$, $(x-1)^3$, $(x-1)^4$, $(x-1)^5$

5. Desarrollando $0 = (1-1)^n$, halla una fórmula nueva.

11 — NUMERO DE SUCESIONES DE p NATURALES CUYA SUMA ES n

a) **Problema.**

He aquí 9 monedas de 20 centavos y 5 alcancías vacías.
¿De cuántas maneras podría distribuir las monedas en las alcancías (considerando que algunas alcancías podrían quedar vacías)?

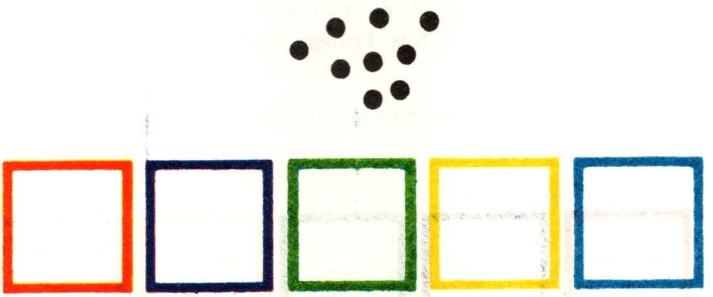


FIG. 28

(Es claro que en este problema no interesa saber cuáles son las monedas colocadas en cada alcancía. Basta conocer el número de monedas que se han colocado en cada una)

Solución :

He aquí una manera de colocar las monedas en las alcancías.

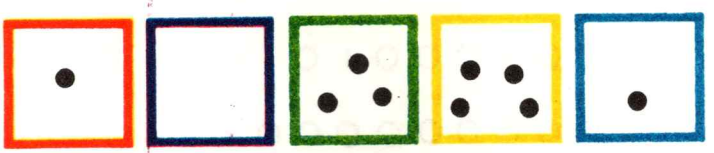


FIG. 29

Consideremos que las alcancías han sido dispuestas de una vez por todas como se indica en el último dibujo. Luego, la situación anterior puede describirse perfectamente mediante el esquema

FIG. 30

o también mediante la "palabra binaria"

O I I O O O I O O O O I O

FIG. 31

Se trata de una "palabra binaria" de 13 cifras que comprende 9 cifras **O** (correspondientes a las 9 monedas) y 4 cifras **I** (luego hay una cifra **I** menos que la cantidad de alcancías).

Escribe la "palabra binaria" definida por la situación siguiente

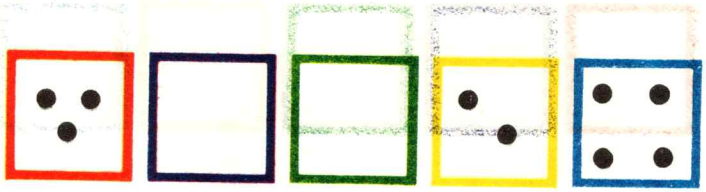


FIG. 32

Representa las situaciones traducidas mediante

O O I O O O I O I O O I O

O O O O O O O O O I I I I

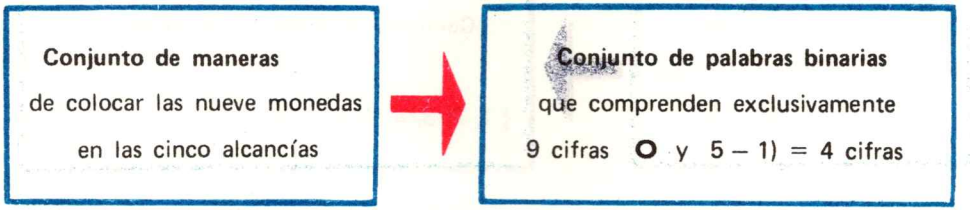
I I O O O O O O O O O I I

O I O I O I O I O O O O O

FIG. 33

¿Mediante qué "palabra binaria" traduces la situación que consiste en poner todas las monedas en la alcancía violeta?

Existe una biyección



Todas estas palabras binarias comprenden 13 signos.

Cada una de esas palabras queda determinada por el lugar que en ella ocupan los O

O I I O O O I O O O O I O → { 1, 4, 5, 6, 8, 9, 10, 11, 13 }

O O I O O O I O I O O I O → { 1, 2, 4, 5, 6, 8, 10, 11, 13 }

O O O O O O O O O I I I I → { 1, 2, 3, 4, 5, 6, 7, 8, 9 }

I I O O O O O O O O O I I → { 3, 4, 5, 6, 7, 8, 9, 10, 11 }

O I O I O I O I O O O O O → { 1, 3, 5, 7, 9, 10, 11, 12, 13 }

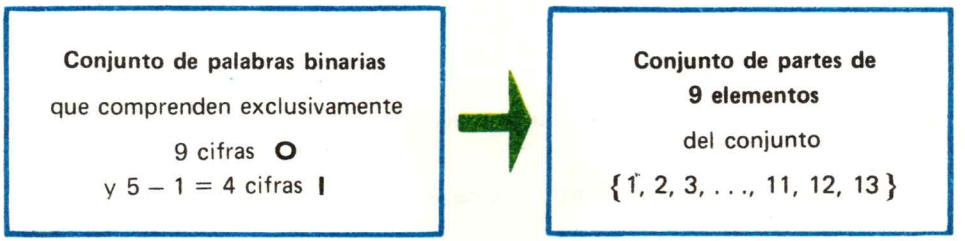
FIG. 34

¿Cuál es la palabra binaria aplicada sobre { 1, 2, 4, 6, 8, 10, 11, 12, 13 } ?

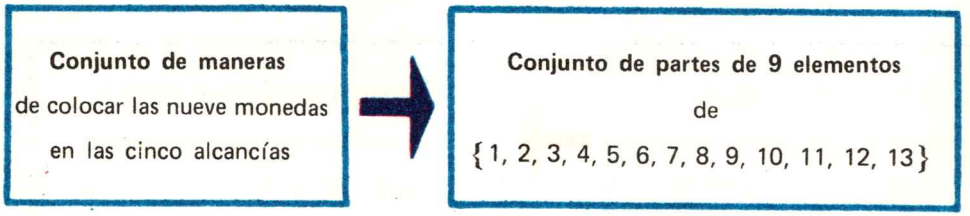
¿Cuál es la **manera** de colocar las monedas en las alcancías

definida por { 2, 3, 4, 6, 8, 9, 10, 12, 13 } ?

Pusimos en evidencia una biyección



De donde resulta la biyección compuesta



El número de maneras de distribuir las nueve monedas en las cinco alcancías es igual al número de partes de 9 elementos de un conjunto de $13 = 9 + 5 - 1$ elementos, es decir

$$\binom{13}{9} = \binom{9 + 5 - 1}{9} = 715$$

b) *GENERALIZACION*

El número de maneras de colocar **n** *monedas de 20 centavos en* **p** *alcancías es igual a*

$$\binom{n + p - 1}{n}$$

c) **Problema**

¿Cuál es el número de sucesiones de **p** *números naturales cuya suma es* **n**?

Solución :

Podríamos haber representado la situación de la figura 30 mediante el término

$$1 + 0 + 3 + 4 + 1$$

Las situaciones que encontramos en a) podrían haber sido designadas por

$$3 + 0 + 0 + 2 + 4$$
$$2 + 3 + 1 + 2 + 1$$
$$9 + 0 + 0 + 0 + 0$$
$$0 + 0 + 9 + 0 + 0$$
$$1 + 1 + 1 + 1 + 5$$

El número de sucesiones de 5 naturales cuya suma es 9 es $\binom{9 + 5 - 1}{9} = \binom{13}{9}$

El número de sucesiones de p naturales cuya suma es n es $\binom{n + p - 1}{n}$

EJERCICIOS

1. El director de un equipo de basket-ball tiene 8 jugadores a su disposición pero sólo puede hacer jugar a 5 simultáneamente.

   ¿De cuántas maneras se puede formar el "cinco" de entrada?

2. $11^0 = 1$

   $11^1 = 11$

   $11^2 = 121$

   $11^3 = 1.331$

   $11^4 = 14.641$

   Estos números se encuentran en el *triángulo de Pascal.*

   Explica utilizando la *fórmula de Newton.*

   Podrías utilizar rápidamente el triángulo de Pascal para calcular 11^5, 11^6, 11^{10}

3. Utilizando el *triángulo de Pascal*, verifica que $9^4 = 10.601 - 4.040 = 6.561$

4. Utilizando la *fórmula de Newton* y el *triángulo de Pascal*, calcula 9^9

5. El profesor de educación física debe dividir su clase de 22 alumnos en dos equipos de fútbol que se enfrentarán.

   ¿De cuántas maneras puede efectuar esta partición?

   (*Respuesta* : 352.716)

6. Un día, un alumno de esa clase está ausente. Se decide formar un equipo de 11 contra un equipo de 10.

   ¿De cuántas maneras se puede efectuar esta partición?

   (*Respuesta* : 352.716)

7. ¿Quieres explicar el porqué de la igualdad de las respuestas de los ejercicios 5 y 6?

8. ¿Cuántas "palabras" de 9 letras distintas puedes formar con las 9 "letras" diferentes $a_1, a_2, a_3, a_4, b_1, b_2, b_3, c_1, c_2$?

– Muy fácil : 9!

– Si suprimo los índices en toda palabra así formada, obtengo una nueva palabra de nueve letras que comprende cuatro a, tres b, y dos c

Así $b_3\, a_2 a_4\, c_1\, c_2\, b_1\, a_3\, b_2\, a_1 \rightarrow b\,a\,a\,c\,c\,b\,a\,b\,a$

Es claro que varias "palabras" en $a_1, a_2, a_3, a_4, b_1, b_2, b_3, c_1, c_2$ originan la misma "palabra" en a, b, c

Demuestra que existen $4! \times 3! \times 2!$ "palabras" en las letras con índices que originan la misma "palabra" en a, b, c

¿Cuántas "palabras" de 9 letras que comprenden cuatro a, tres b y dos c podemos formar?

$$\left(\textit{Respuesta}: \frac{9!}{4! \times 3! \times 2!} = 1.260\right)$$

9. ¿Cuántas "palabras" de $(\alpha + \beta + \gamma + \delta)$ letras que comprenden exactamente α letras a, β letras b, γ letras c, δ letras d?

$$\left(\textit{Respuesta}: \frac{(\alpha + \beta + \gamma + \delta)!}{\alpha!\, \beta!\, \gamma!\, \delta!}\right)$$

10. Sean A y B dos conjuntos finitos tales que $\#\, A = a$ y $\#\, B = b$

Calcula el número de relaciones de A en B

(Recuerda que
"relación de A hacia B" es igual a "parte de $A \times B$")

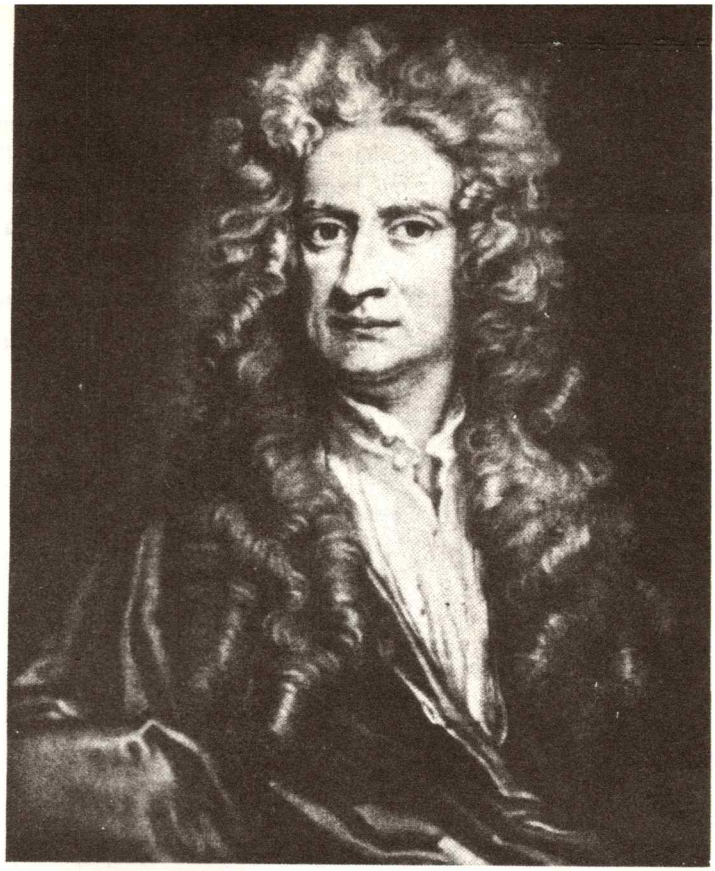
11. ¿Cuántas relaciones definidas en un conjunto de 10 elementos existen?

¿Cuántas de dichas relaciones son transformaciones (o funciones)?

¿Cuántas de esas transformaciones son permutaciones?

(*Respuesta* : 2^{100}, 10^{10}, 10!)

NEWTON (1642-1727)



Isaac Newton, hijo de pequeños granjeros ingleses, no conoció a su padre, quien murió antes de su nacimiento. Muy endeble en sus primeros años, gozó luego de una excelente salud.

A los 19 años, gracias a la influencia de uno de sus tíos que había estudiado en Cambridge, Newton entra a la Universidad como "pair": realiza algunos trabajos para pagar sus estudios. Vive la vida normal de los estudiantes, trabajando y divirtiéndose. Uno de sus profesores es Isaac BARROW, teólogo y excelente matemático que marcaría profundamente la vida de Newton.

En 1665-66, una epidemia de peste bubónica conduce al cierre de la Universidad. Newton se retira con su familia al campo, y durante dos años de meditación solitaria, entre los 23 y 25 años, hace sus más importantes descubrimientos: teoría de las derivadas, leyes de la gravitación, descomposición de la luz. En esta época establece, entre otras cosas, la fórmula de Newton que encontramos en este curso.

BARROW reconoce el genio de Newton y, en un gesto excepcional en la historia de las ciencias, abandona su cátedra en favor de su alumno de 27 años.

A los 30 años Newton es elegido miembro de la Royal Society.

Contrariamente a lo que sucedió a Evaristo Galois, Newton ve el continuo reconocimiento de su talento. Sin embargo, sus contribuciones originales en matemática y física se imponen con dificultad. Siempre fue necesario luchar firmemente para hacer admitir sus nuevas ideas científicas e introducirlas en la enseñanza. Es así como Newton mantiene querellas con dos científicos de Lieja, con el matemático Lucas y con el físico Linus; incapaces de comprenderlo.

En general Newton publicó sus resultados sólo mucho tiempo después de descubrirlos. Bajo la presión de sus amigos publica, a los 45 años, su monumental obra los *"Principia"*, en la que expone la mecánica de manera axiomática.

Después de los 45 años se dedica a la diplomacia y a la política y ocupa un lugar en el Parlamento.

A los 57 años fue nombrado Gran Maestro de Moneda.

No se ocupa de matemática más que de un modo esporádico o para participar en las querellas de prioridad, sobre todo con Leibniz.

LIBRO 2

LA ARITMETICA DE LOS NUMEROS ENTEROS RACIONALES

2

Subgrupos de Z, +

1 – PARTES DE Z , + ESTABLES PARA LA ADICION PARTES DE Z , + ESTABLES PARA LA SUSTRACCION

He aquí el grupo conmutativo **Z** , + de números enteros racionales.

DEFINICION

1) *Una parte* P *de* **Z** *es* **estable para la adición**

ssi

$$\forall a , b \in P : \qquad a + b \in P$$

2) *Una parte* P *de* **Z** *es* **estable para la sustracción**

ssi

$$\forall a , b \in P : \qquad a - b \in P$$

– Define partes de **Z** , + estables para la adición.

– He aquí algunas

$$\omega = \{0, 1, 2, 3, 4, \ldots\}$$

$$1 + \omega = \{1 + n \mid n \in \omega\} = \{1, 2, 3, 4, \ldots\}$$

$$2 + \omega = \{2 + n \mid n \in \omega\} =$$

$$3 + \omega = \qquad\qquad = \{3, 4, 5, \ldots\}$$

$$87 + \omega = \qquad\qquad = \{87, 88, 89, 90, \ldots\}$$

$$2\,\omega = \{2\,n \mid n \in \omega\} = \{0, 2, 4, 6, \ldots\}$$

$$3\,\omega = \{3\,n \mid n \in \omega\} =$$

$$26\,\omega = \qquad\qquad = \{0, 26, 52, 78, \ldots\}$$

$$2\,(1+\omega) = 2+2\omega = \{2\,(1+n) \mid n \in \omega\} = \{2, 4, 6, 8, \ldots\}$$
$$5\,(7+\omega) = \qquad\qquad\qquad\qquad = \{35, 40, 45, \ldots\}$$
$$\{3, 5, 6, 8, 9, 10, 11, \ldots\}$$
$$\{2, 4, 6, 7, 8, 9, \ldots\}$$
$$\{4, 8, 9, 12, 13, 16, 17, 18, 20, 21, 22, 24, 25, 26, 27, 28, \ldots\}$$
$$-\omega = \{0, -1, -2, -3, -4, \ldots\}$$
$$-\omega_0 = \{-1, -2, -3, \ldots\}$$
$$-4-\omega = \{-4, -5, -6, \ldots\}$$
$$-26\,\omega = \{0, -26, -52, \ldots\}$$
$$6\,(-8-\omega) = \{-48, -54, -60, -66, \ldots\}$$

— ¿Estas partes de **Z**, estables para la adición, son también estables para la sustracción?

— Ninguna de estas partes de **Z** es estable para la sustracción.

— Luego existen partes de **Z**, que son estables para la adición, pero no para la sustracción.
Puedes dar partes de **Z** estables para la adición y la sustracción.

— He aquí algunas :

$$\mathbf{Z} = \{0, 1, -1, 2, -2, \ldots\}$$
$$2\,\mathbf{Z} = \{0, 2, -2, 4, -4, 6, -6, \ldots\}$$
$$3\,\mathbf{Z} = \{3z \mid z \in \mathbf{Z}\} = \{0, 3, -3, 6, -6, 9, -9, \ldots\}$$
$$26\,\mathbf{Z} = \{26z \mid z \in \mathbf{Z}\} = \{0, 26, -26, 52, -52, 78, -78, \ldots\}$$
$$0\,\mathbf{Z} = \{0z \mid z \in \mathbf{Z}\} = \{0\}$$

— Todas estas partes de **Z** son **subgrupos** de **Z** , +

¿Qué piensas de la parte vacía de **Z**?

— ϕ es una parte de **Z** estable para la adición y la sustracción.

En efecto

Si $a, b \in \phi$, **Entonces** $a + b \in \phi$ **y** $a - b \in \phi$

— Has dado más arriba algunas partes de **Z** **estables** *para la adición*
y **no estables** *para la sustracción*

¿Quisieras dar ahora una parte de **Z** estable para la sustracción
y no estable para la adición?

– ¿Quisieras dar una parte de **Z** estable para la sustracción, pero que no sea un subgrupo de **Z** , +?

– La parte vacía ϕ de **Z** es estable para + y – pero no es un subgrupo de **Z** , +

– ¿Quisieras dar una **nueva** parte de **Z** estable para – pero que no sea un subgrupo de **Z** , + ?

– ? ? ?

PROPOSICION 1

Si $P \subset \mathbf{Z}$

Entonces

P es un subgrupo de **Z** , +	$\Longleftrightarrow$	$P \neq \phi$ **y** P es estable para –

DEMOSTRACION DE $\Longrightarrow$

Si P es un subgrupo de **Z** , +

Entonces $0 \in P$ y **por lo tanto** $P \neq \phi$

$a, b \in P \Longrightarrow a , -b \in P \Longrightarrow a - b \in P$

luego P es estable para –

l.q.q.d.

DEMOSTRACION DE $\Longleftarrow$

P no es vacío. Sea $a \in P$

P es estable para – Luego $a - a \in P$

$0 \in P$

La parte P comprende el neutro 0 (1)

Si $x \in P$

Entonces $0 \in P$ y $x \in P$

$0 - x \in P$ (P es estable para $-$)

$-x \in P$

La parte P comprende el opuesto de cada uno de sus elementos	(2)

Falta probar que

La parte P es estable para +	(3)

Si $x \in P$, $y \in P$

Entonces $x \in P$, $-y \in P$ (en virtud de (2))

$x - (-y) \in P$ (P es estable para $-$)

$x + y \in P$

l.q.q.d.

EJERCICIOS

1. ¿Quisieras dar partes de **Z** que no sean estables para la adición?

2. Toda parte de **Z** no estable para + es no estable para $-$

3. ¿Las siguientes partes de **Z** son estables para la adición?

$\{-1, 0, 1, 2, 3, \ldots\}$ $\{-2, 0, 2\}$

$\{3, 4, 7\}$ $\{-3, 0, 3, 6, 9, 12, \ldots\}$

$\{3, 8, 5, 13, 14, 18, 16, \ldots\}$ $\{1\}$

4. Si S es un subgrupo de **Z** , + y $a, b, \in S$

Entonces

$a + b \in S$ $\qquad$ $2a - b \in S$

$a - b \in S$ $\qquad$ $(-2)\, a + 3\, b \in S$

$2a + b \in S$ $\qquad$ $(-57)\, a + 26\, b \in S$

5. Si S es un subgrupo de **Z** , +

$a, b \in S \quad ; \quad a', b' \in \mathbf{Z}$

Entonces $a' a + b' b \in S$

6. Si S es un subgrupo de **Z** , +

$a, b, c \in S \; ; \quad a', b', c' \in \mathbf{Z}$

Entonces $a' a + b' b + c' c \in S$

7. Si S es un subgrupo de **Z** , +

$n \in \omega_0 \; ; \quad a_1 , \ldots , a_n \in S \; ; \quad a_1' , \ldots , a_n' \in \mathbf{Z}$

Entonces $a_1' a_1 + a_2' a_2 + \ldots + a_n' a_n \in S$

8. ¿Podrías explicar por qué en algunos ejemplos de partes de **Z** estables para la adición, ciertos números están escritos en **rojo** y otros en **azul**?

9. Los conjuntos de la página 54 en los cuales figuran números azules y rojos, son las menores partes de **Z** que comprenden los números rojos y son estables para +

Observarás que el número azul es el menor natural a partir del cual todos los naturales pertenecen al conjunto.

Fíjate que

$8 = (5 - 1) \times (3 - 1)$

$6 = (2 - 1) \times (7 - 1)$

$24 = (4 - 1) \times (9 - 1)$

10. La parte P de **Z** es estable para + **ssi** $P + P \subset P$

La parte P de **Z** es estable para − **ssi** $P - P \subset P$

11. La parte P de **Z** es un subgrupo de **Z** **ssi** $P - P \subset P \neq \phi$

12. Para toda parte P de **Z** : $P - P \subset P \implies P + P \subset P$

2 — SUBGRUPOS DE Z, + ENGENDRADO POR UNA PARTE P DE Z

He aquí una parte P no vacía de **Z**

y un subgrupo S de **Z** , + que contiene P

$$\phi \neq P \subset S \subset Z$$

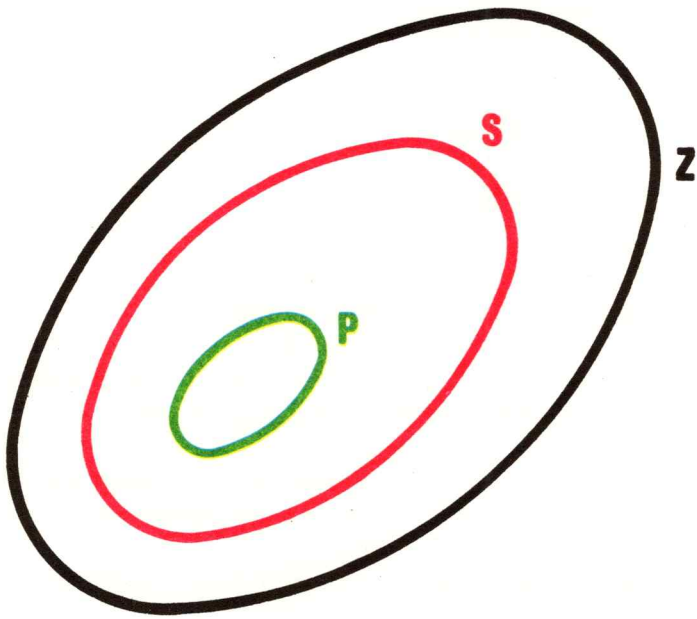


FIG. 35

Si a , b , $c \in P$

Entonces $2a$, $2b$, $2c \in S$

$3a$, $3b$, $3c \in S$

$$\forall\, n \in \omega_0 : \quad na \;,\; nb \;,\; nc \;\in S$$

$$0 = 0a = 0b = 0c \in S$$

$$-a \;,\; -b \;,\; -c \in S$$

$$-2a \;,\; -2b \;,\; -2c \in S$$

$$\forall\, n \in \omega_0 : \quad -na \;,\; -nb \;,\; -nc \in S$$

$$\forall\, z \in \mathbf{Z} : \quad za \;,\; zb \;,\; zc \in S$$

$$\forall\, a', b', c', \in \mathbf{Z} : \quad a'a \;,\; b'b \;,\; c'c \in S$$

$$\forall\, a', b', c', \in \mathbf{Z} : \quad a'a + b'b + c'c \in S$$

DEFINICION

1) **Si** $a_1, \ldots, a_n \;;\; a'_1, \ldots, a'_n \in \mathbf{Z}$

Entonces $a'_1 a_1 + a'_2 a_2 + \ldots + a'_n a_n$ **es una combinación lineal con coeficientes enteros racionales de** $a_1, \ldots, a_n$

2) *Para toda parte no vacía* P *de* **Z** :

se llama **módulo de** P *y se anota mod* P

el conjunto de combinaciones lineales con coeficientes enteros racionales de los elementos de P

Además es $\quad mod\ \phi = \{0\}$

El resultado obtenido aquí arriba se expresa diciendo que

Si el subgrupo S de **Z** , + contiene P

Entonces S ⊃ *mod* P

Todo $p \in P \subset \mathbf{Z}$ es combinación lineal con coeficientes enteros racionales de elementos de P, puesto que $p = 1 \cdot p$

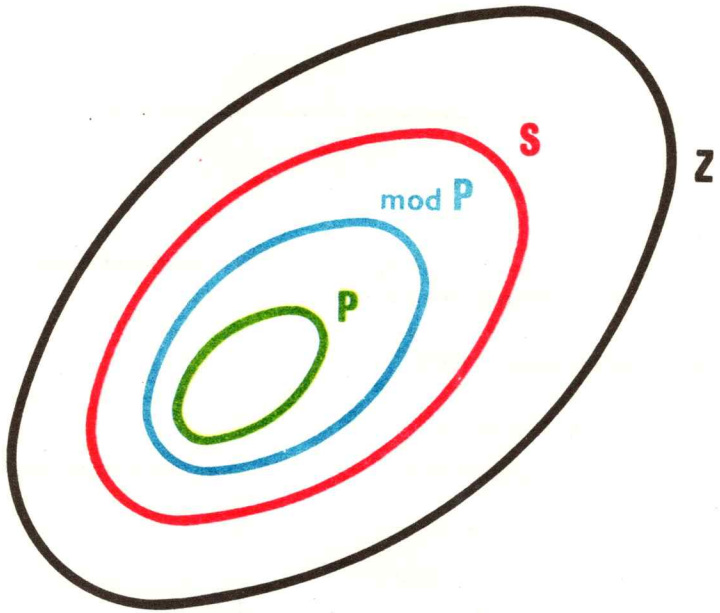
Luego $p \in P \implies p \in mod\ P$

es decir

$$P \subset mod\ P$$

Si el subgrupo S de **Z** , + contiene P

Entonces



P ⊂ mod P ⊂ S

FIG. 36

PROPOSICION 2 — *Para toda parte* P *de* **Z** , +

mod P *es el menor subgrupo de* **Z** , + *que contiene* P

En virtud de lo anterior (fig. p. 55), sólo falta probar que

mod P *es un subgrupo de* **Z** , +

DEMOSTRACION :

Para todo P $\subset$ **Z** : *mod* P $\neq \phi$

En virtud de la proposición 1, para establecer que *mod* P es un subgrupo de **Z** , + basta probar que *la diferencia de toda cupla de elementos de mod* P *pertenece a mod* P, lo cual resulta de la fórmula

$$(a'_1 a_1 + \ldots + a'_n a_n) - (b'_1 b_1 + \ldots + b'_m b_m)$$

$$= a'_1 a_1 + \ldots + a'_n a_n + (-b'_1)\, b_1 + \ldots + (-b'_m)\, b_m$$

DEFINICION — *Para toda parte* P *de* **Z** , +

el menor subgrupo de Z , + que contiene P

se llama también

el subgrupo de Z , + engendrado por P

PROPOSICION 2

Para toda parte P *de* **Z** , +

mod P *es el subgrupo de* **Z** , + *engendrado por* P

DEFINICION

Si $k \in \mathbf{Z}$ y $P \subset \mathbf{Z}$

Entonces $k\,P = \{\, kp \mid p \in P \,\}$

PROPOSICION 3

Si $k \in \mathbf{Z}$ y $P \subset \mathbf{Z}$

Entonces $mod\ kP = k\ mod\ P$

DEMOSTRACION :

$$mod\ P = \{\, a_1 p_1 + \ldots + a_n p_n \mid n \in \omega_0 ; p_1 \ldots p_n \in P;\ a_1 \ldots a_n \in \mathbf{Z} \,\}$$

$$mod\ kP = \{\, a_1 \cdot k\, p_1 + \ldots + a_n \cdot k\, p_n \mid \ldots \,\}$$

$$= \{\, k\,(a_1 p_1 + \ldots + a_n p_n) \mid \ldots \,\}$$

$$= k\ \{\, a_1 p_1 + \ldots + a_n p_n \mid \ldots \,\}$$

$$= k\ mod\ P$$

l.q.q.d.

EJERCICIOS

1. Da 3 elementos de $mod\ \{-2, 8\}$
2. Da 7 elementos de $mod\ \{-15, 12, 30\}$
3. Da un elemento de $\mathbf{Z}$ que no pertenece a $mod\ \{-15, 12, 30\}$
4. $18 \cdot \{-2, 5, 7, 53, 0\ 2040\} = \{-36, 90, 126, 954, 0, 36.720\}$
5. $mod\ 2\omega = 2\ mod\ \omega = 2\mathbf{Z} = mod\ \{2\} = mod\ \{-2\}$
6. $mod\ 3\{7\} = mod\ \{21\} = 3\ mod\ \{7\} = 3 \cdot 7\mathbf{Z} = 21\ \mathbf{Z}$
7. $mod\ \phi = mod\ \{0\} = \{0\} = 0\ \mathbf{Z}$

3 – SUBGRUPO DE Z, + ENGENDRADO POR UN ENTERO RACIONAL

DEFINICION – *Para todo* **k** $\in$ **Z**, *tenemos*

$$\boxed{mod\ k = mod\{k\}}$$

y también se dice que $mod\ k$ *es el* **subgrupo de Z , + engendrado por k**

Es claro que para todo $k \in \mathbf{Z}$:

$$mod\ k = k\mathbf{Z} = \{kz \mid z \in \mathbf{Z}\}$$

PROPOSICION 4

Para todo $a, b \in \mathbf{Z}$: $\boxed{a\,\mathbf{Z} = b\,\mathbf{Z}} \iff \boxed{a = \pm b}$

La implicación $\Longleftarrow$ es evidente.

DEMOSTRACION DE $\Longrightarrow$

He aquí $a, b \in \mathbf{Z}$ tales que $a\,\mathbf{Z} = b\,\mathbf{Z}$

1) **Si** $a\,\mathbf{Z} = b\,\mathbf{Z} = \{0\}$

Entonces $a = b = 0$, de donde $a = \pm b$

2) **Si** $a\,\mathbf{Z} = b\,\mathbf{Z} \neq \{0\}$

Entonces $|a|$ es el menor natural no nulo de $a\mathbf{Z}$

$|b|$ es el menor natural no nulo de $b\mathbf{Z}$

Luego $|a| = |b|$ y $a = \pm b$

l.q.q.d

La proposición 4 también puede formularse :

$$\boxed{\text{Para todo } a, b \in \mathbf{Z} : \quad mod\ a = mod\ b \iff a = \pm b}$$

En particular :

$$\boxed{\text{Para todo } a, b \in \omega : \quad mod\ a = mod\ b \iff a = b}$$

EJERCICIOS

1. $mod\ \mathbf{Z} = \mathbf{Z} = mod\ 1 = mod\ (-1)$

2. $mod\ 0 = \{0\} = mod\ \phi = 0\,\mathbf{Z}$

3. $mod\ 2 = \{z \cdot 2 \mid z \in \mathbf{Z}\} = 2 \cdot \mathbf{Z}$

4. $mod\ 3 = 3\,\mathbf{Z}$; $mod\ 17 = 17\,\mathbf{Z}$; $mod\ 54 = 54\,\mathbf{Z}$

5. $mod\ (-6) = mod\ 6 = 6\,\mathbf{Z}$

6. Para todo $n \in \omega$: $mod\ (-n) = mod\ n$

7. Para todo $z \in \mathbf{Z}$: $mod\ z = z\,\mathbf{Z} = |z| \cdot \mathbf{Z}$

8. $mod\ \{2, 3\} = mod\ 1 = \mathbf{Z}$

9. $mod\ \{4, 8\} = mod\ 4 = 4\,\mathbf{Z}$

10. $mod\ \{12, 18\} = mod\ 6 = 6\,\mathbf{Z}$

11. $mod\ \{48, -84\} = mod\ 12 = 12\,\mathbf{Z}$

12. $mod\ \{4, -7, 13\} =$

13. $mod\ \{8, 12, 28\} =$

14. $mod\ \{10, 28, 70\} =$

15. **Si** S es un subgrupo de $\mathbf{Z}$, + y $s \in \mathbf{Z}$
Entonces $s \in S \iff s\,\mathbf{Z} \subset S$

16. **Si** $P \subset \mathbf{Z}$
Entonces $mod\ P = \{0\} \iff (P = \phi$ **ó** $P = \{0\}$

17. **Si** $a, b, c \in \mathbf{Z}$
Entonces $mod\ \{a, b, c\} = \{a'a + b'b + c'c \mid a', b', c' \in \mathbf{Z}\}$

18. $1 \in P \subset \mathbf{Z} \implies mod\ P = \mathbf{Z}$

19. Para todo $P \subset \mathbf{Z}$:
P es un subgrupo de $\mathbf{Z}$, + $\iff$ $P = mod\ P$

20. Para todo $P \subset \mathbf{Z}$: $mod\ mod\ P = mod\ P$

21. En particular,
$\forall\ P \subset \mathbf{Z}$: $mod\ mod\ P \subset mod\ P$

Dicho de otro modo : Toda combinación lineal (con coeficientes en $\mathbf{Z}$) de combinaciones lineales de elementos de P es una combinación lineal de elementos de P

4 – SUBGRUPOS DE Z , +

Vimos que para todo $k \in \mathbf{Z}$

$$mod\ k = mod\ (-k) = k\ \mathbf{Z} = (-k)\ \mathbf{Z}$$

es el subgrupo de **Z** engendrado por k

Probaremos que los subgrupos $k\mathbf{Z}$ son los únicos subgrupos de **Z** , +

PROPOSICION 5

Si S *es un subgrupo de* **Z** , +

Entonces *existe uno y sólo un natural* $\mathbf{n} \in S$ *tal que* $S = mod\ \mathbf{n}$

Dicho de otro modo :

PROPOSICION 5

Todo subgrupo de **Z** , + *está engendrado por uno y sólo uno de sus naturales.*

DEMOSTRACION :

1) Probemos primero que

todo subgrupo de **Z** , + está engendrado por uno y sólo uno de sus naturales.

He aquí un subgrupo S de **Z**

Luego $0 \in S$

1° **Si** $S = \{0\}$ **Entonces** $S = 0\ \mathbf{Z}$

y el teorema está establecido.

2° **Si** $S \neq \{0\}$

Entonces he aquí un entero racional no nulo $s \in S$

S comprende los enteros racionales no nulos s y $-s$

Luego S comprende por lo menos un natural no nulo.

Llamemos n al menor natural no nulo perteneciente a S

Probemos que $n\ \mathbf{Z} = S$

$\{n\} \subset S$; luego $n\mathbf{Z} = mod\ \{n\} \subset S$ (prop. 2)

Falta establecer que $n\mathbf{Z} \supset S$

es decir

Si $a \in S$ **Entonces** $a \in n\ \mathbf{Z}$

En virtud del teorema de Euclides MM2 , c. 14, § 2, p. 320 ó Introducción del presente libro, p. VIII, existe una y sólo una cupla de enteros racionales b, r tales que $a = bn + r$ y $0 \leqslant r < n$

ó aún $r = a - bn$ y $0 \leqslant a - bn < n$

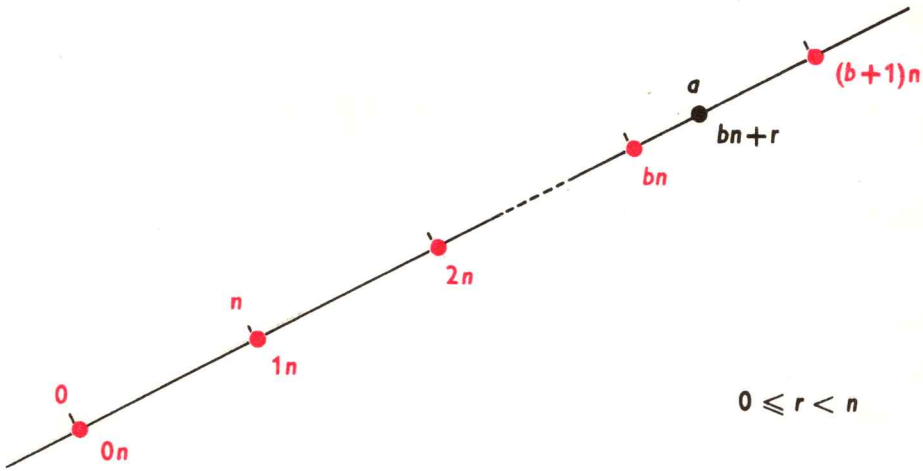


FIG. 37

$a \in S \qquad n \in S$

Luego : $r = 1a - bn \in S$ y $0 \leqslant r < n$

Estas fórmulas muestran que r es un natural de S estrictamente menor que n Pero n es el menor natural no nulo perteneciente a S

Luego $r = 0$ y $a = bn \in n\,Z$

2) Falta probar que todo subgrupo de Z , + está engendrado por uno sólo de sus elementos.

Si cada uno de los naturales n, m engendra el subgrupo S de Z , +

Entonces

$S = n\,Z \quad , \quad S = m\,Z$

$n\,Z = m\,Z$

$n = \pm m$ (Prop. 4)

$n = m$ (puesto que $n, m \in \omega$)

l. q. q. d.

PROPOSICION 6 — *Para toda parte* P *de* **Z**, *existe uno y sólo un natural anotado* $\wedge P$ *tal que*

$$mod\ P = mod \wedge P$$

El natural $\wedge P$ *es combinación lineal, con coeficientes enteros racionales, de elementos de* P

DEMOSTRACION :

He aquí $P \subset \mathbf{Z}$

mod P es un subgrupo de **Z** , + enteramente definido por P

En virtud de la proposición 5, el subgrupo *mod* P está engendrado por uno y sólo un natural. Por lo tanto éste está enteramente definido por P y se anotará $\wedge P$

$\wedge P$ es el único natural tal que $mod\ P = mod \wedge P$

Como $\wedge P \in mod\ P$, el natural $\wedge P$ es combinación lineal con coeficientes enteros racionales de elementos de P

l. q. q. d.

Para toda parte P *de* **Z** , *el natural* $\wedge P$ *está* **definido** *por*

$$mod\ P = mod \wedge P$$

PROPOSICION 7

Si $k \in \mathbf{Z}$ y $P \subset \mathbf{Z}$

Entonces $\wedge kP = |k| \wedge P$

DEMOSTRACION :

$$\begin{aligned} mod \wedge kP &= mod\ kP && \text{(Prop. 6)} \\ &= k\ mod P && \text{(Prop. 3)} \\ &= k\ mod \wedge P && \text{(Prop. 6)} \\ &= mod\ k \wedge P && \text{(Prop. 3)} \\ &= mod\ |k| \cdot \wedge P && \text{(Prop. 4)} \end{aligned}$$

Luego $mod \wedge kP = mod\ |k| \wedge P$

Como $\wedge kP \in \omega$ y $|k| \wedge P \in \omega$

Se deduce (prop. 4)

$$\wedge kP = |k| \wedge P$$

l. q. q. d.

El teorema siguiente reúne todos los resultados de este capítulo, y es lo único que debe retenerse.

TEOREMA

Todo subgrupo de Z, + está engendrado por uno y sólo uno de sus naturales.

De ahí que para toda parte P de Z, existe uno y sólo un natural, anotado $\wedge$ P tal que mod P = mod $\wedge$ P

El natural $\wedge$ P es combinación lineal, con coeficientes enteros racionales, de elementos de P y

Para todo $z \in Z$: $\wedge zP = |z| \cdot \wedge P$

EJERCICIOS

1. $\wedge\{2\} =$
2. $\wedge\{-2\} =$
3. $\wedge\{2, 4\} =$
4. $\wedge\{6, 10\} =$
5. $\wedge\{-2, 3\} =$
6. $\wedge\phi = 0$
7. $\wedge\omega =$
8. $\wedge Z =$
9. $\wedge 2Z =$
10. $\wedge\{-2{,}5\} =$
11. $\wedge\{-18, 12, 30\} =$
12. $\wedge 2\omega =$
13. $\wedge(-\omega) =$
14. $\wedge\{0\} =$
15. $\wedge 3Z =$
16. $\wedge\{48, -54\} =$
17. $\wedge\{4, -7, 13\} =$
18. $\wedge\{8, 12, -25\} =$
19. $\wedge\{10, 25, 70\} =$
20. Si $I \in P \subset Z$
    Entonces $\wedge P = 1$

3

Más alto común divisor
Más bajo común múltiplo

1 – LA RELACION DIVIDE EN Z

DEFINICION — Para todo $a, b \in \mathbf{Z}$

$a \mid b$ **ssi** $\exists\, q \in \mathbf{Z} :$ $b = aq$

Expresiones sinónimas

$a \mid b$

a **divide** b

a es (un) **divisor** de b

b es (un) **múltiplo** de a

a (es) **más bajo** que b

b (es) **más alto** que a

Se indica que a no divide b, escribiendo $a \nmid b$

EJEMPLOS

1. $2 \mid 18 \;;\; 25 \mid -625 \;;\; -7 \mid 56 \;;\; -12 \mid -84$

$1 \mid 7 \;;\; 1 \mid -100 \;;\; -1 \mid 48 \;;\; -1 \mid -26$

2. $\forall z \in \mathbf{Z} \;:\; 1 \mid z \text{ y } -1 \mid z$

3. $18 \mid 18 \;;\; -189 \mid -189 \;;\; 215 \mid 215 \;;\; 0 \mid 0$

4. Para todo $z \in \mathbf{Z}$: $z \mid z$ ... puesto que $z = z \cdot 1$

5. La relación | definida en **Z** no es reflexiva.

6. El número 1 es más bajo que todo entero racional.

El número -1 es más bajo que todo entero racional.

7. $1 \mid -1 \text{ y } -1 \mid 1$

8. La relación | definida en **Z no es antisimétrica.**

9. $15 \mid -15 \;,\; 0 \mid -0 \;,\; -0 \mid 0 \;,\; -15 \mid 15$

10. $\forall z \in \mathbf{Z} \;:\; z \mid z \;;\; -z \mid -z \;;\; z \mid -z \;;\; -z \mid z$

11. $63 \mid 0$ puesto que $0 = 0 \times 63$

12. $184 \mid 0 \;;\; (-1965) \mid 0 \;;\; 0 \mid 0$

13. Para todo $z \in \mathbf{Z}$: $z \mid 0$

14. 0 es más alto que todo entero racional.

15. **Si** $0 \mid z \in \mathbf{Z}$

Entonces existe $z' \in \mathbf{Z}$ tal que $0\,z' = z$ y $z = 0$

16. 0 es el único entero racional más alto que todo entero racional.

17. $5 \nmid 1 \;,\; 1 \mid 5$

18. La relación | definida en **Z** **no es simétrica.**

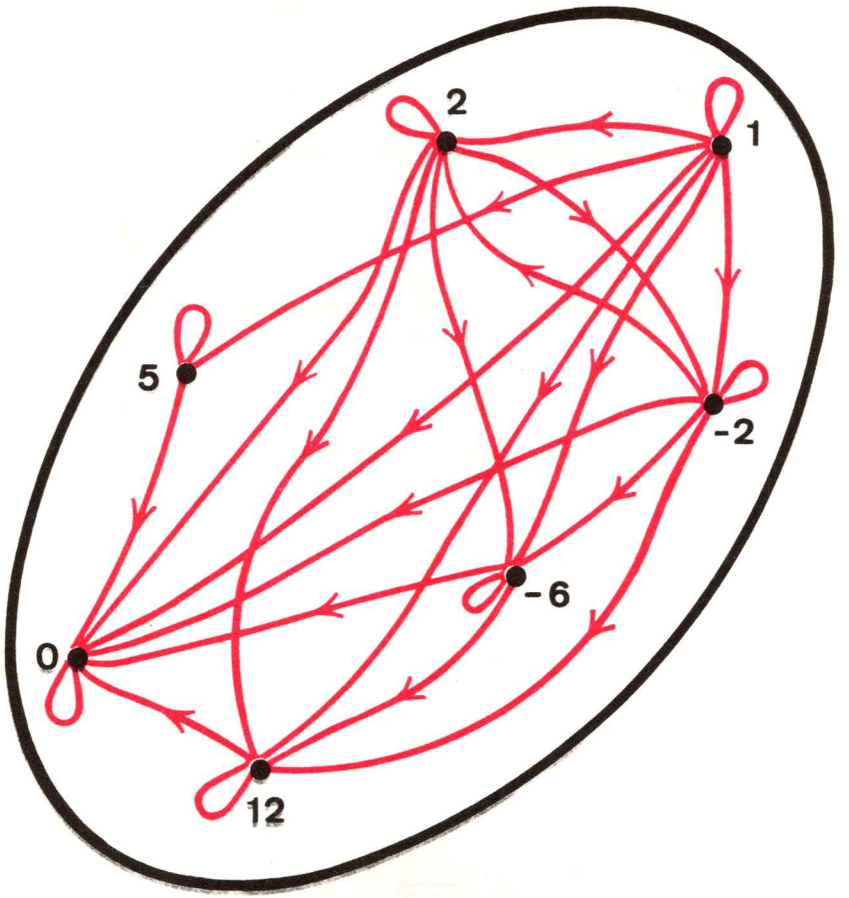
19. $2 \nmid 3 \qquad 3 \nmid 2$

20. La relación | definida en **Z** no es total.

21. $\forall\, a,b \in \mathbf{Z}$:

$$a \mid b \iff a \mid -b \iff -a \mid b \iff -a \mid -b \iff |a| \mid |b|$$

22.



UN ESQUEMA DE LA RELACION | EN EL CONJUNTO $\{0, 1, 2, -2, 5, -6, 12\}$

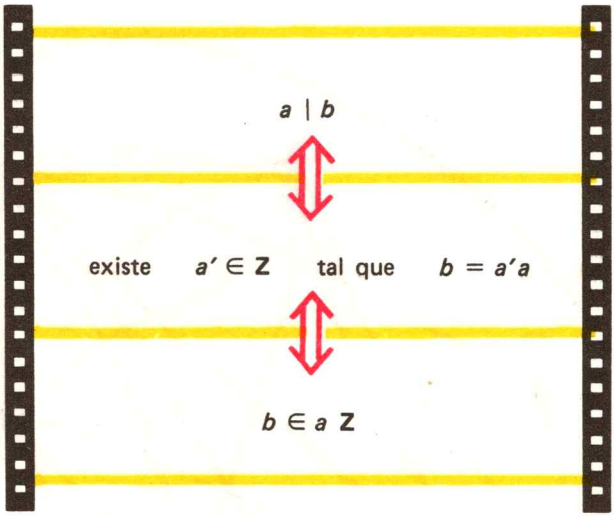
FIG. 38

PROPOSICION 1

Para todo $a, b \in \mathbf{Z}$:

$$a \mid b \iff b \in a\mathbf{Z} \iff b\mathbf{Z} \subset a\mathbf{Z}$$

DEMOSTRACION DE $\mathbf{a \mid b \iff b \in aZ}$



DEMOSTRACION DE $\mathbf{b \in aZ \implies bZ \subset aZ}$

Si $b \in a\mathbf{Z}$

Entonces $a\mathbf{Z}$ es un subgrupo de $\mathbf{Z}$, + que comprende b

Pero $b\mathbf{Z}$ es el menor subgrupo de $\mathbf{Z}$, + que comprende b

Luego $b\mathbf{Z} \subset a\mathbf{Z}$

DEMOSTRACION DE $\mathbf{bZ \subset aZ \implies b \in aZ}$

$b \in b\mathbf{Z} \subset a\mathbf{Z}$ implica $b \in a\mathbf{Z}$

l. q. q. d.

PROPOSICION 2

La relación | *definida en* **Z** *es reflexiva y transitiva.*

No es ni simétrica, ni antisimétrica,

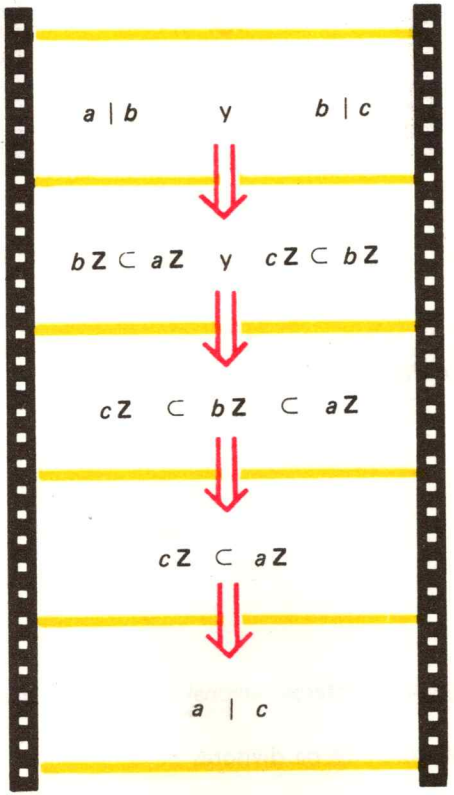
pero para todo $a, b \in \mathbf{Z}$: $(a|b \quad \text{y} \quad b|a) \iff a = \pm b$

Luego resulta que :

La relación | *definida en* ω *es un orden.*

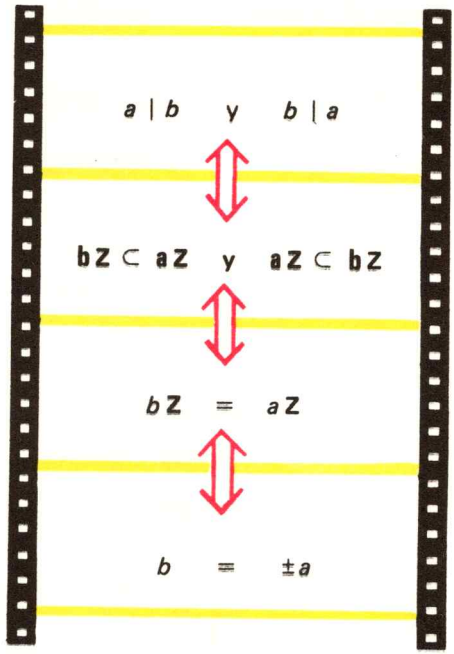
Ya se estableció la reflexividad de | y se observó que esta relación no es ni simétrica, ni antisimétrica.

DEMOSTRACION DE **la transitividad de la relación** |



l. q. q. d

DEMOSTRACION DE $(a \mid b \quad y \quad b \mid a) \iff a = \pm b$



(C. 2, prop. 4)

l. q. q. d.

Problema :

¿Qué se puede decir de $z \in Z$ *sabiendo que* $z|1$ *?*

Solución :

$$(z \mid 1 \quad y \quad 1 \mid z) \iff z = \pm 1$$ (Prop. 2)

Consecuencias :

1) 1 y -1 son los únicos enteros racionales más bajos que todo entero racional.

2) $\{1, -1\}$ es el conjunto de divisores de 1

3) $\{1, -1\}$ es el conjunto de divisores de -1

EJERCICIOS

1. SI $0 \neq a \in \mathbf{Z}$ y $b \in \mathbf{Z}$

Entonces $a \mid b \iff \frac{b}{a} \in \mathbf{Z}$

DEMOSTRACION DE $\Longrightarrow$

$a \mid b$

$\Downarrow$

$b = a'a$ y $a' \in \mathbf{Z}$

$\Downarrow$

$\frac{b}{a} = \frac{a'a}{a} = a' \in \mathbf{Z}$

$\Downarrow$

$\frac{b}{a} \in \mathbf{Z}$

DEMOSTRACION DE $\Longleftarrow$

$\frac{b}{a} \in \mathbf{Z}$

$\Downarrow$

$\frac{b}{a} = a' \in \mathbf{Z}$

$\Downarrow$

$b = \left(\frac{b}{a}\right) \cdot a = a'a$ y $a' \in \mathbf{Z}$

$\Downarrow$

$a \mid b$

l. q. q. d.

2. Establece la transitividad de la relación divide definida en **Z** basándote exclusivamente en la definición de dicha relación.

3. $\forall\, a, b \in \mathbf{Z}$: $(\, a|b$ y $b|a\,) \iff |a| = |b|$

2 — CONJUNTOS DE DIVISORES DE UNA PARTE DE Z

DEFINICION — *He aquí una parte* P *de* Z

Se llaman **divisores de P,** *a los enteros racionales que dividen todos los elementos de* P

Se designa con div P *al conjunto de divisores de* P

$$div\ P \quad = \quad \{ \quad z \in Z \quad \blacksquare \quad \forall\, p \in P : z \mid p \quad \}$$

En el caso de conjuntos unitarios se simplificanla anotación escribiendo,

para todo $z \in Z$: $\quad div\ z \quad = \quad div \{ z \}$

EJEMPLOS

1. $div \{ 2, -2, 4, -26 \} = \{ 1, -1, 2, -2 \} = div\ 2 = div\ (-2)$

2. $div \{ 12, -18 \} = \{ 1, -1, 2, -2, 3, -3, 6, -6 \} = div\ 6 = div\ (-6)$

3. $div\ 14 = \{ 1, -1, 2, -2, 7, -7, 14, -14 \} = div\ (-14)$

4. $div\ 5 = \{ 1, -1, 5, -5 \} = div\ (-5)$

5. $div\ 0 = Z = div\ \phi$

6. $div\ Z = \{ 1, -1 \}$

7. $div \{ 8, -15 \} = \{ 1, -1 \}$

8. $div\ 1 = \{ 1, -1 \} = div\ (-1)$

9. $\forall P \subset \mathbf{Z} \quad : \quad \{ 1, -1 \} \subset div\ P$

10. $\forall z \in \mathbf{Z} \quad : \quad \{ 1, -1, z, -z \} \subset div\ z$

11. $\forall z \in \mathbf{Z} \quad : \quad div\ z = div\ (-z) = div|z|$

12. $\forall n \in \omega \quad :$ $\omega \cap div\ n$ es el conjunto de divisores naturales de n

13. $\forall a, b \in \mathbf{Z} \quad : \quad a \mid b \iff a \in divb$

14. $\forall a \in \mathbf{Z} \quad : \quad diva = div(-a) = div|a|$

PROPOSICION 3

Para todo a b $\in \mathbf{Z}$

$$a \mid b \iff a \in div\ b \iff div\ a \subset div\ b$$

DEMOSTRACION :

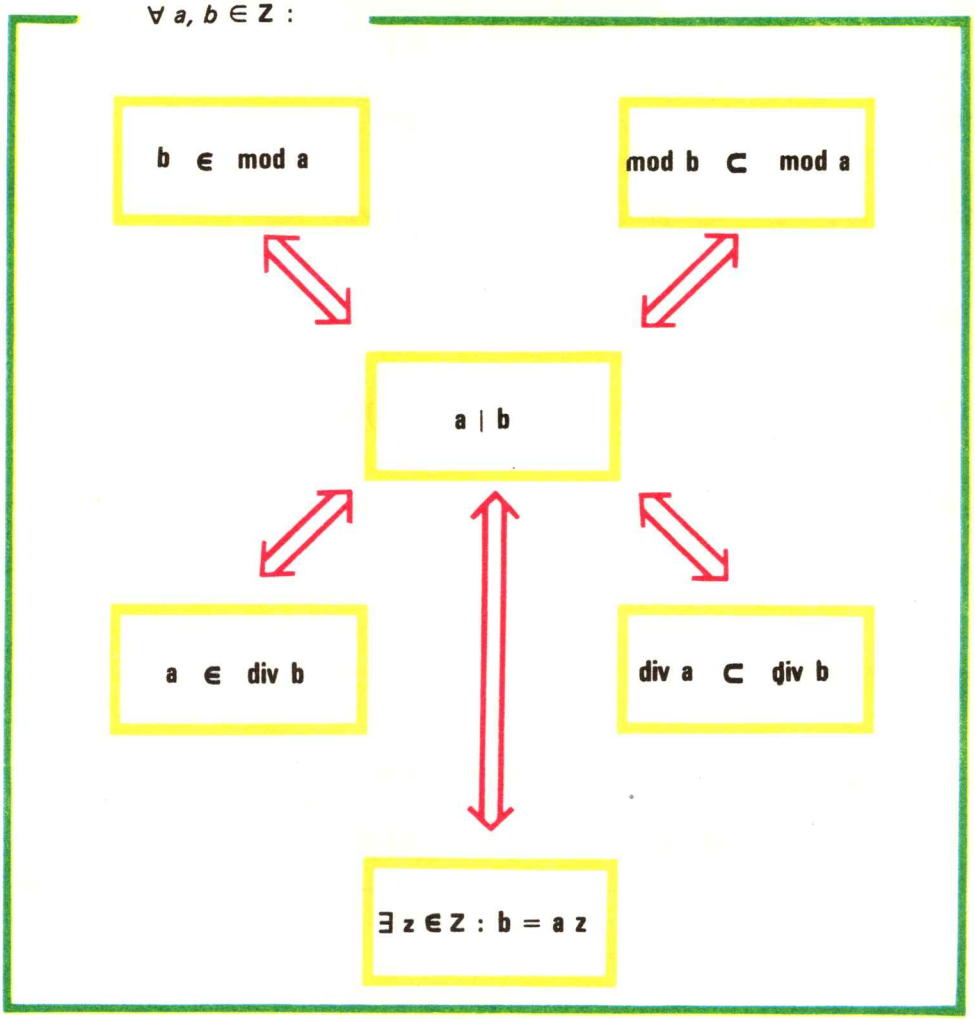
La primera equivalencia resulta de la definición de *div b*

La transitividad de la relación | implica

$$a \mid b \implies divaa \subset divb$$

Finalmente, $a \in diva \subset divb$ implica $a \mid b$

l.q.q.d.



CINCO MANERAS DE EXPRESAR QUE **a** DIVIDE **b** FIG. 39

Consecuencia

Para todo $a, b \in \mathbf{Z}$:

$$div\ a = div\ b \iff a \mid b \ \text{ y } \ b \mid a \overset{\text{prop. 2}}{\iff} b = \pm a$$

En particular :

Para todo $m, n \in \omega$: $\quad div\ m = div\ n \iff m = n$

1) Para todo $a, b \in \mathbb{R}$, la fórmula $\boxed{a \leqslant b}$
se lee "a menor que b"

2) Para todo $a, b \in \mathbb{R}$, la fórmula $\boxed{a < b}$
se lee "a estrictamente menor que b"

3) Para toda cupla de conjuntos A, B, la fórmula $\boxed{A \subset B}$
se lee "A menor que B"

4) Para todo $a, b \in \mathbb{Z}$, la fórmula $\boxed{a \mid b}$
se lee "a más bajo que b"

EJERCICIOS

1. $div\ 2\mathbb{Z} =$

2. $div\ \omega =$

3. $div\ (-4\omega) =$

4. $div\ (16 + 8\omega) =$

5. La relación | definida en $\mathbb{Z}$ no es un orden

6. **Si** $a, b \in \mathbb{Z}$
Entonces $div\ a = div\ b \iff |a| = |b|$

7. **Si** $A, B \subset \mathbb{Z}$ **Entonces** $div\ (A \cup B) = div\ A \cap div\ B$

8. **Si** $a, b \in \mathbb{Z}$ **Entonces** $div\ \{a, b\} = div\ a \cap div\ b$

9. **Si** $A, B, C \subset \mathbb{Z}$ **Entonces** $div\ (A \cup B \cup C) = div\ A \cap div\ B \cap div\ C$

10. **Si** $a, b, c \in \mathbb{Z}$ **Entonces** $div\ \{a, b, c\} = div\ a \cap div\ b \cap div\ c$

11. $n \in \omega$: n es el más alto elemento de $\omega \cap div\ n$

12. $n \in \omega_0$: n es el más alto elemento y el elemento más grande de $\omega \cap div\ n$

13. 0 es el menor elemento de $\omega \cap div\ 0$
0 es el más alto elemento de $\omega \cap div\ 0$

3 — COMPARACION DE LOS ORDENES $\leqslant$ y | DEFINIDOS SOBRE ω_0

PROPOSICION 4

Las relaciones $\leqslant$ *y* | *definidas sobre* ω_0 *son* **órdenes.**

El orden $\leqslant$ *es total; el orden* | *no es total.*

Además

$$| \quad \subset \quad \leqslant$$

Dicho de otro modo :

$\forall a, b \in \omega_0$: $\quad a \mid b \implies a \leqslant b$

DEMOSTRACION ;

1°) La relación $\leqslant$ es un orden total definido sobre R y por lo tanto sobre $\omega_0 \subset R$

2°) La proposición 2 nos enseña que | es un orden sobre ωyy por lo tanto sobre $\omega_0 \subset \omega$
Este orden no es total puesto que $2 \nmid 3 \nmid 2$

3°) **Si** $\quad a \mid b \quad$ y $\quad a, b \in \omega_0$

Entonces $\quad b = aq \quad$ con $\quad q \in \omega_0$

Luego $\quad q \geqslant 1 \quad$ y $\quad b = aq \geqslant a \cdot 1 = a$

l. q. q. d

Consecuencia

Para todo $n \in \omega_0$: $\quad \#(\omega \cap div\ n) \leqslant n$

EJERCICIOS

1. 0 es el menor elemento del conjunto totalmente ordenado ω , $\leqslant$ que no comprende un mayor elemento.

2. 0 es el mayor elemento del conjunto totalmente ordenado $-\omega$, $\leqslant$ que no comprende un menor elemento.

3. El conjunto totalmente ordenado $\mathbf{Z}$, $\leqslant$ no comprende ni un menor ni un mayor elemento.

4. **Si** el conjunto E comprende por lo menos dos elementos distintos,

   Entonces $\mathcal{P}$E, $\subset$ es un conjunto ordenado, pero no totalmente ordenado, cuyo menor elemento es ϕ y cuyo mayor elemento es E

5. $2 \not< 3$ y $3 \not< 2$ y $2 \leqslant 3$

   2 es estrictamente menor que 3

   2 no es ni más bajo ni más alto que 3

6. 1 es el más bajo y 0 es el más alto elemento del conjunto ordenado ω , | que no es un conjunto totalmente ordenado.

7. $\forall P \subset \mathbf{Z} : \quad a \in div\ P \iff -a \in div\ P$

8. $\forall P \subset \mathbf{Z} : \quad 0 \in div\ P \iff (P = \phi \text{ o } P = \{0\})$

9. $\forall z \in \mathbf{Z} : \quad \#(div\ z \cap \omega) \leqslant |z|$

10. $\forall z \in \mathbf{Z} : \quad z = -z \iff z = 0$

11. **Si** $z \in \mathbf{Z}_0$

    Entonces $\#\ div\ z = 2 \cdot \#(\omega \cap div\ z) \in 2\ \omega_0$

12. **Si** la parte P de $\mathbf{Z}$ no es ni ϕ, ni $\{0\}$

    Entonces $\#div$ P es un número natural par.

13. ¿Qué puedes decir de $-\omega$, | ?

4 — MAS ALTO COMUN DIVISOR

PROPOSICION 5

Si $A \subset B \subset \mathbf{Z}$

Entonces $div A \supset div B$

DEMOSTRACION :

Si $d \in div B$

Entonces d divide todos los elementos de B

d divide todos los elementos de A (puesto que $A \subset B$)

d es un divisor de A

$d \in div A$

Todo divisor de B es un divisor de A

$div A \supset div B$

l. q. q. d

PROPOSICION 6

Si $a_1, \ldots, a_n, d, a'_1, \ldots, a'_n \in \mathbf{Z}$

Entonces $d \mid a_1, \ldots, d \mid a_n \Longrightarrow d \mid a'_1 a_1 + \ldots + a'_n a_n$

DEMOSTRACION :

Si $d \mid a_1, \ldots, d \mid a_n$

Entonces $a_1 = dq_1, \ldots, a_n = dq_n$ (con $q_1, \ldots q_n \in \mathbf{Z}$)

$$a'_1 a_1 + \ldots + a'_n a_n$$

$$= a'_1 dq_1 + \ldots + a'_n dq_n = d(a'_1 q_1 + \ldots + a'_n q_n)$$

de donde $d \mid a'_1 a_1 + \ldots + a'_n a_n$

l. q. q. d.

Acabamos de probar que todo divisor de P es un divisor de toda combinación lineal, con coeficientes enteros racionales, de elementos de P.

Es decir, todo divisor de P es un divisor de *mod* P;
de donde resulta la reformulación de la

PROPOSICION 6

$$\forall P \subset \mathbf{Z} : \qquad div\ P \quad \subset \quad div\ mod\ P$$

PROPOSICION 7

$$\forall P \subset \mathbf{Z} : \qquad div\ P \quad = \quad div\ mod\ P$$

DEMOSTRACION :

Acabamos de establecer que $div\ P \subset div\ mod\ P$

Por otra parte, $P \subset mod\ P \Longrightarrow div\ P \supset div\ mod\ P$
prop. 5

l. q. q. d.

TEOREMA

Para todo P $\subset$ Z , el natural $\wedge$ P está definido por cada una de las fórmulas

$$mod\ P = mod \wedge P \qquad (1)$$

$$div\ P = div \wedge P \qquad (2)$$

DEMOSTRACION :

El teorema del capítulo 2 establece que la fórmula (1) define $\wedge$ P

La fórmula (2) **es verdadera** porque

$$div\ P = div\ mod\ P \qquad \text{(prop. 7)}$$

$$= div\ mod \wedge P \qquad \text{(fórmula (1))}$$

$$= div \wedge P \qquad \text{(prop. 7)}$$

En virtud de la fórmula final del § 2, la igualdad $div\ P = div \wedge P$ define el número natural $\wedge$ P

l. q. q. d.

PROPOSICION 8

Para toda parte P *de* **Z** : $\wedge$ P *es el más alto número natural perteneciente a div* P

Si $\{0\} \neq P \neq \phi$ **Entonces** $\wedge$ P *es el mayor número natural perteneciente a div* P

DEMOSTRACION :

1° En virtud del teorema (p. 83)

$$\wedge P \in div \wedge P = div\ P$$

de donde $\wedge P \in div\ P$

Acabamos de probar que $\wedge P$ es un natural perteneciente a *div* P

He aquí un natural *n* perteneciente a *div* P

Luego $n \in div\ P = div \wedge P$, de donde $n \in div \wedge P$; es decir $n \mid \wedge P$

Todo natural *n* perteneciente a *div* P , divide $\wedge P$

$\wedge$ P es el más alto natural perteneciente a *div* P

2° **Si** $\{0\} \neq P \neq \phi$

Entonces $0 \notin div\ P$

En virtud de la proposición 4,

$\wedge P$ es el mayor natural perteneciente a *div* P

Esta proposición permite que llamemos a $\wedge P$
el **más alto común divisor** *de los elementos de* P

En forma abreviada : $\wedge P$ es el m. a. c. d. (de los elementos) de P

EJERCICIOS

1. $div\,\{18, 60\} = \{\ldots\}$
   $\wedge\,\{18, 60\} =$
2. $div\,\{2.100, 5.040, 5.880\} = \{\ldots\}$
3. $\wedge\,div\,\{2.100, 5.040, 5.880\} =$
3. $\wedge\,\{2.100, 5.040\} =$
4. $\wedge\,\{5.040, 5.880\} =$
5. $\wedge\,\{2.100, 5.880\} =$
6. $\wedge\,\{12, 18\} =$
7. $\wedge\,\{12, 24\} =$
8. $\wedge\,\{84, 24\} =$
9. $\wedge\,\{60, 24\} =$
10. $\wedge\,\{45, 0\} = 45$
11. $\wedge\,\{-45, 0\} = 45$
12. $mod\ \phi = \{0\}$
13. $mod\ \phi = mod\ 0$
14. $div\ \phi = div\ 0 = \mathbf{Z}$
15. $\wedge\,\phi = 0$
16. $mod\ \{0\} = \{0\}$
17. $mod\ \{0\} = mod\ 0$
18. $div\ \{0\} = div\ 0$
19. $\wedge\,\{0\} = 0$
20. **Si** $P \subset \mathbf{Z}$
    Entonces $mod\ P = \{0\} \iff mod\ P = mod\ 0 \iff div\ P = div\ 0$
21. **Si** $P \subset \mathbf{Z}$
    Entonces $\wedge P = 0 \iff P = \phi$ o $P = \{0\}$
22. He aquí $P \subset \mathbf{Z}$
    div P es el conjunto de números enteros racionales que son más bajos que todo elemento de P
    $\wedge$P es el más alto número natural perteneciente a *div* P

$\wedge$P es el más alto número natural que es más bajo que todo elemento de P

5 – CALCULO DEL MAS ALTO COMUN DIVISOR DE UNA CUPLA DE ENTEROS RACIONALES

DEFINICION

$\forall\, a, b \in \mathbf{Z}$: $\qquad a \wedge b \;=\; \wedge \{a, b\}$

El **natural** $a \wedge b$ se llama más alto común divisor de a y b (en realidad es el más alto de los divisores comunes naturales de a, b)

De manera abreviada : $a \wedge b$ *es el* m.a.c.d. *de* **a** *y* **b**

En virtud del teorema (§ 4, p. 83) de este capítulo, $a \wedge b$ está **definido** por cada una de las fórmulas

$$div\,(a \wedge b) \;=\; div\,\{a, b\} \qquad (1)$$

$$mod\,(a \wedge b) \;=\; mod\,\{a, b\} \qquad (2)$$

Es claro que $\forall\, a, b \in \mathbf{Z}$: $\qquad a \wedge b \;=\; b \wedge a$

La proposición siguiente nos permitirá calcular el m.a.c.d. de toda cupla de enteros racionales.

PROPOSICION 9

1) $\forall\, a, b \in \mathbf{Z}$: $\qquad a \wedge b \;=\; |a| < |b|$

2) **Si** **r** *designa el resto de la división euclídea del número natural* **a** *por el número natural* **no nulo b**

Entonces $\qquad a \wedge b \;=\; b \wedge r$

DEMOSTRACION :

1 — Para todo $a, b \in \mathbf{Z}$:

$$div(a \wedge b) = div\{a, b\} \qquad \text{(fórmula (2))}$$

$$= diva \cap divb$$

$$= div|a| \cap div|b| = div(|a| \wedge |b|)$$

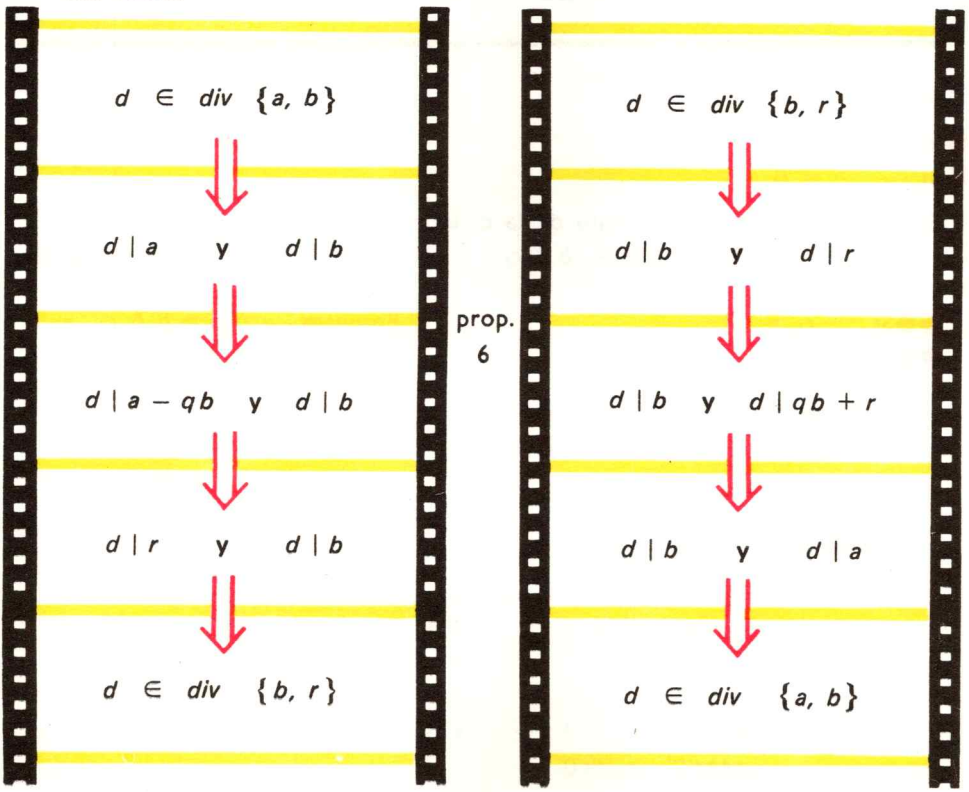
De donde $a \wedge b = |a| \wedge |b|$ (4)

2 — Llamemos q al cociente y r al resto de la división euclídea del natural a por el natural no nulo b

$$a = qb + r \qquad 0 \leqslant r < b$$

$$a - qb = r$$

Los filmes



establecen que $div\{a, b\} = div\{b, r\}$

De donde, en virtud del teorema (p. 83),

$$\begin{aligned} div \wedge \{a, b\} &= div \{a, b\} = div \{b, r\} = div \wedge \{b, r\} \\ div \wedge \{a, b\} &= div \wedge \{b, r\} \\ \wedge \{a, b\} &= \wedge \{b, r\} \\ a \wedge b &= b \wedge r \end{aligned}$$

l. q. q. d.

La primera parte de la proposición 9 reduce la búsqueda del m. a. c. d. de toda cupla de enteros racionales al cálculo del m. a. c. d. de una cupla de naturales.

Si uno de los naturales es nulo,

Entonces $div\ a \wedge 0 = div\{a, 0\} = div\ a$, de donde $a \wedge 0 = a$

Problema

He aquí $a, b \in \omega$

Busquemos un **método para calcular** $a \wedge b$

Solución :

● **Si** $b = 0$ **Entonces** $a \wedge b = a$

● **Si** $b \neq 0$

Entonces llamaremos r_1 al resto de la división euclídea de a por b

$a \wedge b = b \wedge r_1 \qquad b > r_1 \geqslant 0$ (prop. 9)

●● **Si** $r_1 = 0$ **Entonces** $a \wedge b = b \wedge r_1 = b$

●● **Si** $r_1 \neq 0$

Entonces llamemos r_2 al resto de la división de b por r_1

$a \wedge b = b \wedge r_1 = r_1 \wedge r_2 \qquad b > r_1 > r_2 \geqslant 0$

●●● **Si** $r_2 = 0$ **Entonces** $a \wedge b = b \wedge r_1 = r_1 \wedge r_2 = r_1$

●●● **Si** $r_2 \neq 0$

Entonces llamemos r_3 al resto de la división de r_1 por r_2

$a \wedge b = b \wedge r_1 = r_1 \wedge r_2 = r_2 \wedge r_3$

$b > r_1 > r_2 > r_3 \geqslant 0$

•••• **Si** $r_3 = 0$ **Entonces** $a \wedge b = \ldots = r_2 \wedge r_3 = r_2$

•••• **Si** $r_3 \neq 0$

Entonces etc. . . .

$$b > r_1 > r_2 > r_3 > \ldots \geqslant 0$$

es una sucesión estrictamente decreciente de números naturales.

Se obtiene un resto nulo después de un número finito de etapas.

Llamemos r_n a ese resto nulo.

.....Entonces $a \wedge b = b \wedge r_1 = r_1 \wedge r_2 = \ldots = r_{n-1} \wedge r_n = r_{n-1} \wedge 0 = r_{n-1}$

Disposición práctica

	q_1	q_2	q_3	q_4	. . .	q_{n-1}	q_n
a	b	r_1	r_2	r_3		r_{n-2}	$r_{n-1} = a \wedge b$
q_1 b	q_2 r_1	q_3 r_2	q_4 r_3	q_5 r_4		q_n r_{n-1}	
r_1	r_2	r_3	r_4	r_5		$r_n = 0$	

	1	1	1	1	12	1	7
12936	7800	5136	2664	2472	192	168	24
7800	5136	2664	2472	2304	168	168	
5136	2664	2472	192	168	24	0	

$$12936 \wedge 7800 = 24$$

EJERCICIOS

1. El m.a.c.d. de enteros naturales define la ley interna de ω

$\omega \times \omega \rightarrow \omega : \quad (a, b) \rightarrow a \wedge b$

Esta ley es conmutativa.

Para todo $a \in \omega$: $\quad a \wedge 0 = a = 0 \wedge a$

Luego 0 es **neutro** para $\wedge$

Para todo $a \in \omega$: $\quad a \wedge 1 = 1 = a \wedge 1$

Lo cual se expresa diciendo que 1 es **absorbente** para $\wedge$

2. Calcula :

$238 \wedge 322$ $\qquad$ $48.048 \wedge 96.144$

$7035 \wedge 6125$ $\qquad$ $1428 \wedge 746$

3. Para todo $a, b \in \mathbf{Z}$, existen $a', b' \in \mathbf{Z}$ tales que

$$a'a + b'b = a \wedge b$$

4. Si $\quad a, b \in \mathbf{Z}$

Entonces $\quad a \wedge b = (-a) \wedge b = a \wedge (-b) = (-a) \wedge (-b) = |a| \wedge |b|$

5. $\quad a, b, k \in \mathbf{Z}$: $\quad ka \wedge kb = |k| \cdot a \wedge b$

6. Si $\quad a, b, n \in \omega$

Entonces $\quad \boxed{na \wedge nb = n \cdot a \wedge b}$

7. **Si** $a, b \in \mathbf{Z}$, $n \in \omega_0$, $n \mid a$, $n \mid b$

Entonces

$$\frac{a}{n} \wedge \frac{b}{n} = \frac{a \wedge b}{n}$$

8. **Si** $a, b \in \mathbf{Z}$ y $(a \neq 0$ ó $b \neq 0)$

Entonces

$$\frac{a}{a \wedge b} \wedge \frac{b}{a \wedge b} = 1$$

9. En virtud de la proposición 8,

Si uno de los enteros racionales a, b es no nulo

Entonces $a \wedge b$ es el mayor natural que divide a la vez a a y b (lo cual justifica parcialmente la expresión "máximo común divisor" utilizada clásicamente).

10. $0 \wedge 0 = 0$ es el más alto común divisor natural de 0 y 0 y no es el máximo común divisor natural de 0 y 0

6 — MAS BAJO COMUN MULTIPLO

PROPOSICION 10

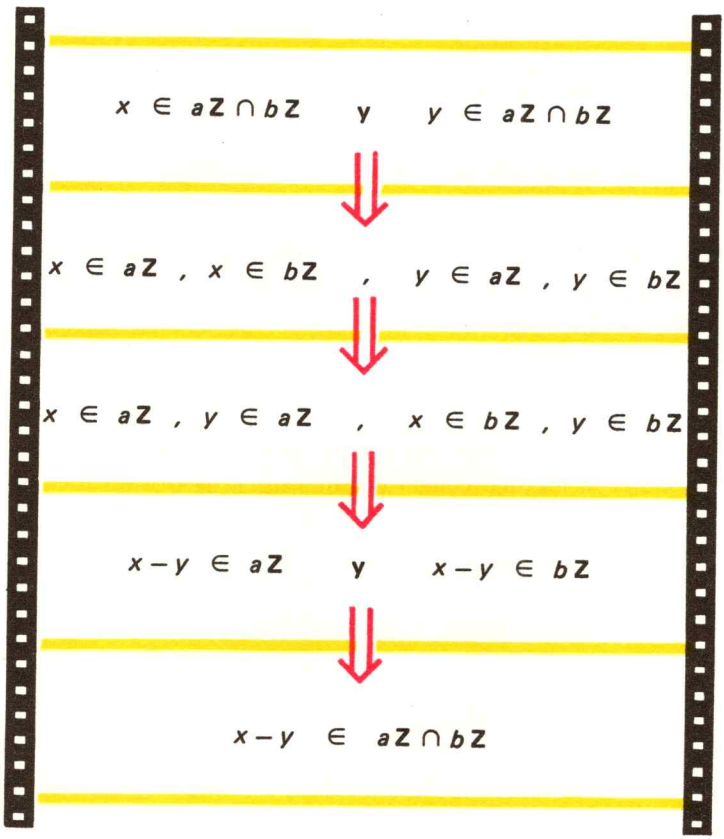
1) $\forall a, b \in \mathbf{Z}$: $a\mathbf{Z} \cap b\mathbf{Z}$ es subgrupo de $\mathbf{Z}$, +

2) *De ahí que para todo* $\mathbf{a}, \mathbf{b} \in \mathbf{Z}$, *existe uno y sólo un natural que se anota* $\mathbf{a} \vee \mathbf{b}$ *tal que* $\mathbf{aZ} \cap \mathbf{bZ} = (\mathbf{a} \vee \mathbf{b})\,\mathbf{Z}$

3) *El número* $\mathbf{a} \vee \mathbf{b}$ *es el más bajo natural que es a la vez múltiplo de* **a** *y* **b** (*En forma abreviada* : m.b.c.m. de **a** y **b**)

DEMOSTRACION :

1) En virtud de la proposición 1 del c. 2, basta establecer que $a\mathbf{Z} \cap b\mathbf{Z}$ es estable para la sustracción.



2) Todo subgrupo de $\mathbf{Z}$, + está engendrado por uno y sólo uno de sus naturales (c. 2, teorema p. 68).

Por lo tanto, para todo $a, b \in \mathbf{Z}$, existe uno y sólo un natural, que anotaremos $a \vee b$

tal que $$a\mathbf{Z} \cap b\mathbf{Z} = (a \vee b)\,\mathbf{Z}$$

3) *Mostremos primero que el natural* **a** $\vee$ **b** *es más alto que* **a** *y* **b**

$$a \vee b \in (a \vee b)\mathbf{Z} = a\mathbf{Z} \cap b\mathbf{Z}$$

$$a \vee b \in a\mathbf{Z} \; ; \; a \vee b \in b\mathbf{Z}$$

$$a \mid a \vee b \; ; \; b \mid a \vee b$$

He aquí un natural **m**, *múltiplo de* **a** *y* **b**

Probemos que **a** $\vee$ **b** *es más bajo que* **m**

$$a \mid m \qquad\qquad b \mid m$$

$$m \in a\mathbf{Z} \qquad\qquad m \in b\mathbf{Z}$$

$$m \in a\mathbf{Z} \cap b\mathbf{Z}$$

$$m \in (a \vee b)\,\mathbf{Z}$$

$$a \vee b \mid m$$

$a \vee b$ es por lo tanto el número más bajo que es a la vez múltiplo de a y b

EJERCICIOS

1. $2\mathbf{Z} \cap 3\mathbf{Z} = 6\mathbf{Z}$ **luego** $2 \vee 3 = 6$

2. $12\mathbf{Z} \cap 18\mathbf{Z} = 36\mathbf{Z}$ **luego** $12 \vee 18 = 36$

3. Para todo $a \in \mathbf{Z}$: $a\mathbf{Z} \cap 0\mathbf{Z} = 0\mathbf{Z}$
   luego $a \vee 0 = 0$

4. Para todo $a \in \mathbf{Z}$: $a\mathbf{Z} \cap 1\mathbf{Z} = |a|\,\mathbf{Z}$

luego $a \vee 1 = |a|$

5. Para todo $a, b \in \mathbf{Z}$: $a \vee b = b \vee a$

6. Para todo $a \in \mathbf{Z}$: $a \vee a = |a|$

7. Para todo $a, b \in \mathbf{Z}$: $a \vee b = (-a) \vee b = a \vee (-b) = (-a) \vee (-b) = |a| \vee |b|$

El cálculo del m.b.c.m. de una cupla de enteros racionales se reduce, pues, al cálculo del m.b.c.m. de una cupla de enteros naturales.

8. **Si** por lo menos uno de los enteros racionales a y b es distinto de 1

Entonces $a \vee b$ es el menor múltiplo común natural de a y b (lo cual justifica parcialmente la expresión "mínimo común múltiplo" utilizada tradicionalmente).

9. $1 \vee 1 = 1$ es el más bajo múltiplo natural común de 1 y 1

0 es el menor natural que es a la vez múltiplo de 1 y de 1

4

Factorizaciones primas de los números naturales

1 — ENTEROS RACIONALES PRIMOS ENTRE SI

DEFINICION — *Para todo* $a, b \in \mathbf{Z}$:

a y b son **primos entre sí** $\iff$ $a \wedge b = 1$

EJEMPLOS

$17 \wedge 13 = 1$; $(-13) \wedge 25 = 1$; $(-26) \wedge (-127) = 1$

Para todo $z \in \mathbf{Z}$: $1 \wedge z = 1 = (-1) \wedge z$

PROPOSICION 1

Si $\mathbf{a, b, c \in Z}$

Entonces $\mathbf{a \wedge b = 1}$ y $\mathbf{a \mid bc} \implies \mathbf{a \mid c}$

DEMOSTRACION :

Sabemos que (c. 2, teorema, p. 68)

$$a \wedge b = a'a + b'b \qquad (\text{con } a', b' \in \mathbf{Z})$$

Luego existen $a', b' \in \mathbf{Z}$ tales que

$$a'\,a + b'.b = 1$$

de donde

$$\begin{aligned} c &= c\,a'\,a + c\,b'\,b \\ &= c\,a' \cdot a + b' \cdot b\,c \end{aligned}$$

Pero

$$a \mid a \qquad \text{y} \qquad a \mid b\,c$$

Luego

$$a \mid c\,a' \cdot a + b' \cdot b\,c \qquad \text{(c. 3, proposición 6, p. 82)}$$

$$a \mid c$$

l. q. q. d.

EJERCICIOS

1. Si $a, b, c, d \in \omega_0$ y $a \wedge b = 1 = c \wedge d$

Entonces $\boxed{a\,d = b\,c} \iff \boxed{a = c \quad \text{y} \quad b = d}$

2. Si $a, b, c, d \in \omega_0$ y $a \wedge b = 1 = c \wedge d$

Entonces $\boxed{\frac{a}{b} = \frac{c}{d}} \iff \boxed{a = c \quad \text{y} \quad b = d}$

3. Si $a, b \in \omega_0$

Entonces existe una y sólo una cupla $(p, q) \in \omega_0 \times \omega_0$ tal que :

$$\boxed{\frac{a}{b} = \frac{p}{q} \qquad \text{y} \qquad p \wedge q = 1}$$

Pasar de $\frac{a}{b}$ a $\frac{p}{q}$ es *"reducir* $\frac{a}{b}$ *a su más simple expresión"*.

2 – ENTEROS RACIONALES PRIMOS

$$\begin{aligned} \#\, div\ 0 &= \#\mathbf{Z} = \delta \\ \#\, div\ 1 &= \#\{1, -1\} = 2 \\ \#\, div\ (-1) &= \#\{1, -1\} = 2 \end{aligned}$$

Si $z \in \mathbf{Z} \setminus \{0, 1, -1\}$

Entonces $\#\{1, -1, z, -z\} = 4$ y $\{1, -1, z, -z\} \subset div\ z$

Luego $\#\, div\ z \geqslant 4$

DEFINICION – *Para todo* $z \in \mathbf{Z}$:

$$z \text{ primo} \iff \#\, div\ z = 4$$

EJEMPLOS

1. Los enteros racionales 0, 1, −1 no son **primos.**
2. Los enteros racionales 2 y −2, 3 y −3 son primos.
3. Los enteros racionales 4, −4, 6, −6, 84, −125 no son primos.
4. Sabemos que para todo $z \in \mathbf{Z}$: $div\ z = div\ (-z) = div\ |z|$
   Luego, para todo $z \in \mathbf{Z}$: z primo $\iff$ $-z$ primo $\iff$ $|z|$ primo
5. Para todo $z \in \mathbf{Z}$: z primo $\iff$ $\#(\omega \cap div\ z) = 2$
6. El natural p es primo
   ssi
   El cardinal del conjunto de sus divisores naturales es 2
   ssi
   Para todo natural n tal que $1 < n < p$: $n \nmid p$
   ssi
   Para todo natural n tal que $1 < n < p$: $\frac{p}{n} \notin \omega$
7. Los enteros racionales
   $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, \ldots$
   $-2, -3, -5, -7, -11, -13, -17, -19, -23, -29, -31, -37, -41, \ldots$
   son primos.
8. Todo natural primo es estrictamente mayor que 1
9. **Si** $p_1, \ldots, p_n$ son naturales primos
   Entonces $p_1 \cdot p_2 \cdot \ldots \cdot p_n > 1$

P ROPOSICION 2

Si $p, q \in \mathbf{Z}$

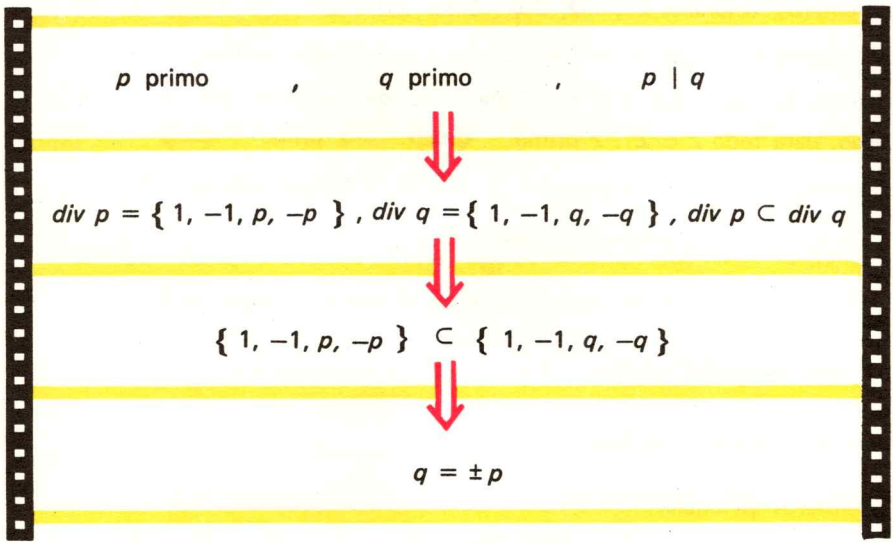
Entonces p primo, q primo, $p \mid q$ $\Longrightarrow$ $q = \pm p$

En particular

Si $p, q \in \omega$

Entonces p primo, q primo, $p \mid q$ $\Longrightarrow$ $p = q$

DEMOSTRACION :



l. q. q. d.

De esta proposición resulta que

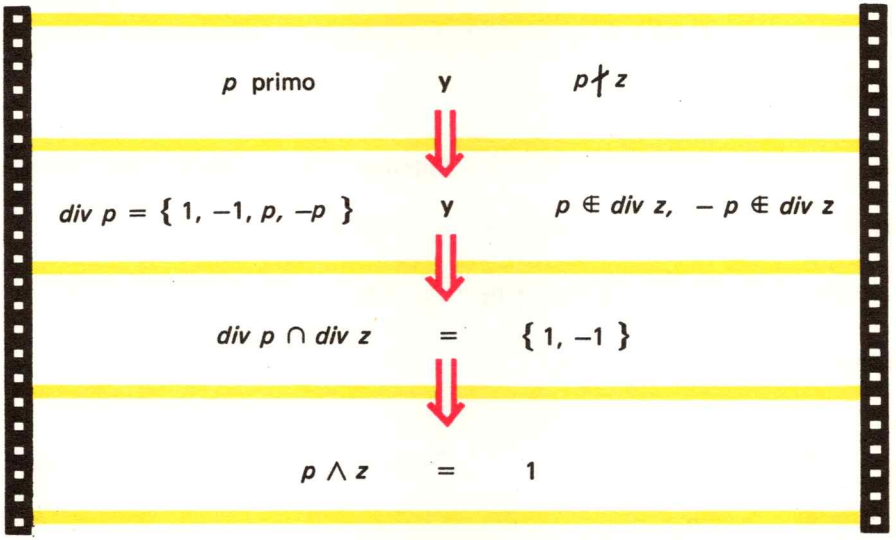
Si p, q designan naturales primos distintos **Entonces** $p \nmid q$

PROPOSICION 3

Si $p, z \in \mathbf{Z}$

Entonces p primo y $p \nmid z \implies p \wedge z = 1$

DEMOSTRACION :



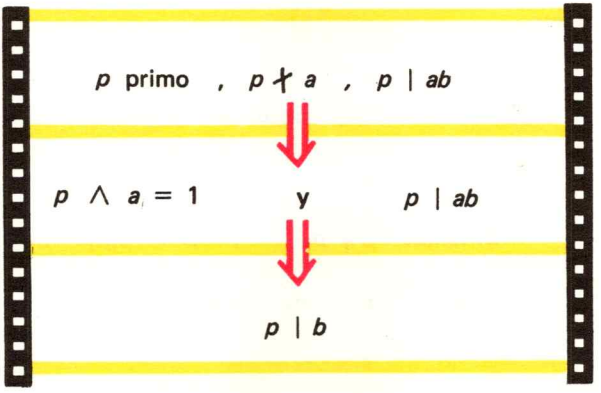
l. q. q. d.

PROPOSICION 4

Si $p, a, b \in \omega$

Entonces p primo, $p \mid ab$, $p \nmid a \implies p \mid b$

DEMOSTRACION :



prop. 3

prop. 1

l. q. q. d.

PROPOSICION 5

Si $p, p_1, \ldots, p_n$ *designan naturales primos,*

Entonces $p \mid p_1 \cdot p_2 \cdot \ldots \cdot p_n \implies$ p es igual a uno de los p_i

DEMOSTRACION :

- **Si** $p = p_1$ **Entonces** la proposición queda establecida.
- **Si** $p \neq p_1$

  Entonces $p \nmid p_1$ y $p \mid p_1 \cdot p_2 \cdot \ldots \cdot p_n$

  Luego $p \mid p_2 \cdot \ldots \cdot p_n$

  - **Si** $p = p_2$ **Entonces** la proposición queda establecida.
  - **Si** $p \neq p_2$

    Entonces $p \nmid p_2$ y $p \mid p_2 \cdot p_3 \cdot \ldots \cdot p_n$

    Luego $p \mid p_3 \cdot \ldots \cdot p_n$

    - **Si** $p = p_3$ **Entonces** la proposición queda establecida.
    - etc. . . .

      - **Si** $p = p_{n-1}$ **Entonces** la proposición queda establecida.
      - **Si** $p = p_{n-1}$

        Entonces $p \nmid p_{n-1}$ y $p \mid p_{n-1} \cdot p_n$

        Luego $p \mid p_n$ de dohde $p = p_n$ y la proposición queda establecida.

l. q. q. d.

PROPOSICION 6

Todo natural distinto de 1 *es divisible por un natural primo.*

DEMOSTRACION :

He aquí un natural $n \neq 1$

Si $n = 0$

Entonces $2 \mid n$ y la proposición queda establecida.

Supongamos, pues, que $0 \neq n \neq 1$

Llamemos D al conjunto de naturales distintos de 1 que dividen n

El conjunto D no es vacío, puesto que $1 \neq n \in D$

Designemos con p al menor natural perteneciente a D

$$p \mid n$$

Probemos que **p** *es primo.*

Si p no fuese primo,

Entonces p sería divisible por un natural d tal que

$$1 < d < p$$

pero $1 \neq d \mid p \mid n \implies 1 \neq d \mid n$

de donde $d \in D$ y p no sería el menor natural perteneciente a D

luego p es primo.

l. q. q. d.

TEOREMA 1

El conjunto de números naturales primos es infinito.

Basta establecer que para todo $n \in \omega$, existe un natural primo $p > n$

DEMOSTRACION :

Sea $m = n! + 1 = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (n-1) \cdot n + 1$

He aquí un natural d

Si $d \mid m$ y $d \leqslant n$ **Entonces** $d \mid m$ y $d \mid n!$

Luego $d \mid m - n!$ es decir $d \mid 1$ y $d = 1$

Por lo tanto hemos probado que

$m = n! + 1$ no es divisible por ningún natural k tal que $1 < k \leqslant n$

Bien, en virtud de la proposición 6, existe un natural primo p

tal que $p \mid m$ luego $p > n$

l. q. q. d.

DEFINICION

Se llama **factorización prima** *de un número natural a toda expresión de ese natural como producto de naturales primos. Se dice que dos factorizaciones primas son iguales ssi difieren sólo en el orden de sus factores.*

EJEMPLOS

1. Los números 0 y 1 no admiten ninguna factorización prima.

2. 2 X 3 X 3 es una factorización prima de 18

3. 2 X 3 X 3 , 3 X 2 X 3 , 3 X 3 X 2 designan la misma factorización prima de 18

4. 7 es una factorización prima de 7

THÉORÈME 2

Todo natural n distinto de 0 y de 1 admite una y sólo una factorización prima.

TEOREMA DE LA FACTORIZACION PRIMA DE LOS NATURALES

1°) Existencia

- **Si** n es primo **Entonces** n es una factorización prima.
- **Si** n no es primo

Entonces existe un natural primo p_1 tal que $p_1 \mid n$

Sea $n = p_1 q_1$ de donde $1 < q_1 < n$

- **Si** q_1 es primo **Entonces** $n = p_1 q_1$ es una factorización prima.
- **Si** q_1 no es primo,

Entonces existe un natural primo p_2 tal que $p_2 \mid q_1$

Sea $q_1 = p_2 q_2$ de donde $1 < q_2 < q_1$

- **Si** q_2 es primo **Entonces** $n = p_1 p_2 q_2$ es una factorización prima.
- etc. . . .

El procedimiento que acabamos de describir continúa cada vez que se encuentra un q_i no primo.

Ahora bien, $n > q_1 > q_2 > \ldots$ es una sucesión estrictamente decreciente de naturales.

Por lo tanto esta sucesión es finita.

Su último elemento, que anotaremos q_i , es primo.

Luego $n = p_1 p_2 \ldots p_i q_i$ es una factorización prima.

2°) Unicidad

He aquí dos factorizaciones primas del número n

$$n = p_1 p_2 \ldots p_h = q_1 q_2 \ldots q_k$$

Sin restringir la generalidad, podemos suponer $h \leqslant k$

$$p_1 \mid q_1 q_2 \ldots q_k$$

En virtud de la proposición 5, p_1 es igual a uno de los q
Cambiemos eventualmente la numeración de los q de modo de obtener

$$p_1 = q_1$$

Luego

$$p_1 p_2 \ldots p_h = p_1 q_1 \ldots q_k$$

$$p_2 \ldots p_h = q_2 \ldots q_k$$

$$p_2 \mid q_2 \ldots q_k$$

En virtud de la proposición 5, p_1 es igual a uno de los $q_2, \ldots, q_k$
Cambiemos eventualmente la numeración de los $q_2, \ldots, q_k$ de modo de obtener

$$p_2 = q_2$$

Luego

$$p_2 p_3 \ldots p_h = p_2 q_3 \ldots q_k$$

$$p_3 \ldots p_h = q_3 \ldots q_k$$

$$p_3 \mid q_3 \ldots q_k$$

Y así siguiendo.

Se obtiene sucesivamente

$$p_1 = q_1 \ , \ p_2 = q_2 \ , \ldots , \ p_h = q_h$$

Si $k = h$ **Entonces** el teorema está demostrado.

Si $k > h$ **Entonces** se tendría $p_1 \ldots p_h = p_1 \ldots p_h q_{h+1} \ldots q_k$

$$1 = q_{h+1} \ldots q_k$$

Lo cual es imposible, puesto que ningún producto de números naturales primos es 1

l. q. q. d.

EJERCICIOS

1. El conjunto de números naturales primos es numerable.

2. El conjunto de números enteros racionales primos es numerable.

3. He aquí un natural n distinto de 0 y de 1

   n primo $\iff$ n no es divisible por ningún natural primo $p < n$

4. Criba de Eratóstenes.

   En la lista de números naturales de 1 a 100
   tacha primero el número 1 que no es primo.

   El número 2 es primo.

   Los múltiplos de 2 distintos de 2 no son primos. Táchalos.

   Es seguro que el primer número no tachado es seguramente primo. Es 3.

   Los múltiplos de 3 distintos de 3 no son primos. Táchalos.

   El primer número no tachado es primo. Es 5

   etc.

   Mediante este procedimiento construirás la sucesión de naturales primos comprendidos entre 1 y 100

5. Cuáles son las factorizaciones primas de los números

   24, 56, 79, 101, 144, 211, 564, 324, 1.024, 625, 1.000, 1.000.000

6. Gracias a la criba de Eratóstenes se puede dar la sucesión estrictamente creciente de números naturales primos.

   Para hallar la factorización prima de un número natural, primeramente se trata de dividirlo por 2 tantas veces como sea posible. Luego por 3, por 5, etc.

Ejemplo :

720	2
360	2
180	2
90	2
45	3
15	3
5	5
1	

$720 = 2 \times 2 \times 2 \times 2 \times 3 \times 3 \times 5$

7. Designemos con P el conjunto de los números naturales primos de ω

Para todo $n \in \omega$, representemos mediante $p(n)$ al conjunto de divisores primos de n. Luego se tiene

$$\begin{aligned} p(n) &= \{x \in \mathrm{P} \mid x \mid n\} \\ p(0) &= \mathrm{P} \\ p(1) &= \phi \end{aligned}$$

La anotación $p(n)$, define la aplicación

$$p : \omega \to \mathcal{P}\mathrm{P} \quad : \quad n \to p(n)$$

La función p aplica ω, sobre el conjunto de partes finitas de P
Dos naturales distintos pueden tener la misma imagen por p

$$p(6) = p(12) = p(48) = p(18) = \{2, 3\}$$

Si a, b designan naturales

Entonces

$$a \mid b \iff p(a) \subset p(b)$$

$$p(1) \subset p(a) \subset p(0)$$

$$a \wedge b = 1 \iff p(a) \cap p(b) = \phi$$

Para todo natural $n \neq 0$, designemos mediante $sp(n)$ el producto de los números primos de $p(n)$
Luego se tiene $sp(48) = sp(12) = sp(6) = 6$

$$sp(a) \mid sp(b) \iff p(a) \subset p(b)$$

8. **Si** p_1, p_2 designan naturales primos distintos,

Entonces para todo $n_1, n_2 \in \omega$: $p_1^{n_1} \wedge p_2^{n_2} = 1$

9. **Si** $p_1, \ldots, p_k$ designan naturales primos distintos dos a dos y los a_i, b_i designan naturales,

Entonces

$$p_1^{a_1} \ldots p_k^{a_k} = p_1^{b_1} \ldots p_k^{b_k} \iff \text{para todo } i \in \{1,\ldots,k\}: a_i = b_i$$

$$p_1^{a_1} \ldots p_k^{a_k} = 1 \iff \text{todos los } a_i \text{ son nulos.}$$

10. **Si** $p_1, \ldots, p_k$ designan naturales primos distintos dos a dos y los a_i designan naturales,

Entonces

$$\begin{aligned} p_1^{a_1} \wedge p_2^{a_2} \ldots p_k^{a_k} &= 1 \\ p_2^{a_2} \wedge p_3^{a_3} \ldots p_k^{a_k} &= 1 \\ p_{k-1}^{a_{k-1}} \wedge p_k^{a_k} &= 1 \end{aligned}$$

5

ω , $\wedge$, $\vee$, |

1 – M.A.C.D. , M.B.C.M. Y FACTORIZACIONES PRIMAS

He aquí un natural a (distinto de 0 y de 1) dado por su factorización prima

$$a = 5 \cdot 3 \cdot 2 \cdot 7 \cdot 2 \cdot 2 \cdot 3 \cdot 11 \cdot 5 \cdot 17 \cdot 11 \cdot 11$$

Es más claro expresar esta factorización bajo la forma

$$a = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 \cdot 5 \cdot 7 \cdot 11 \cdot 11 \cdot 11 \cdot 17$$

o mejor aún, utilizando los exponentes,

$$a = 2^3 \cdot 3^2 \cdot 5^2 \cdot 7 \cdot 11^3 \cdot 17$$

De manera general, todo natural n distinto de 0 y de 1 se escribe

$$n = {p_1}^{n_1} \cdot {p_2}^{n_2} \cdot \ldots \cdot {p_h}^{n_h}$$

donde los p_i son naturales primos distintos dos a dos, y los n_i son naturales no nulos.

Y también, utilizando el subterfugio de los exponentes nulos, los naturales b, c distintos de 0 y de 1, se escribirán

$$b = {p_1}^{b_1} \cdot {p_2}^{b_2} \cdot \ldots \cdot {p_k}^{b_k}$$

$$c = {p_1}^{c_1} \cdot {p_2}^{c_2} \cdot \ldots \cdot {p_k}^{c_k}$$

donde los p_i son naturales primos distintos dos a dos

los b_i son naturales, no todos nulos

los c_i son naturales, no todos nulos

Resulta,

$$bc = {p_1}^{b_1+c_1} \cdot {p_2}^{b_2+c_2} \cdot \ldots \cdot {p_k}^{b_k+c_k}$$

De donde la

PROPOSICION 1

Si $s = p_1^{s_1} \cdot p_2^{s_2} \cdot \ldots \cdot p_k^{s_k}$ y $t = p_1^{t_1} \cdot p_2^{t_2} \cdot \ldots \cdot p_k^{t_k}$

donde los p_i son naturales primos distintos dos a dos, los s_i y los t_i son naturales,

Entonces $s \mid t \iff$ para todo $i \in \{1, 2, \ldots, k\}$: $s_i \leqslant t_i$

EJEMPLOS

1. $1.400 = 2^3 \cdot 5^2 \cdot 7$
   $2.268 = 2^2 \cdot 3^4 \cdot 7$

   $1.400 = 2^3 \cdot 3^0 \cdot 5^2 \cdot 7^1$
   $2.268 = 2^2 \cdot 3^4 \cdot 5^0 \cdot 7^1$
   $1 = 2^0 \cdot 3^0 \cdot 5^0 \cdot 7^0$

2. $1.400 \nmid 2.268$ puesto que ... $3 > 2$

3. $\omega \cap div\ 1.400 = \{ 2^u \cdot 5^v \cdot 7^w \mid u \in \{0, 1, 2, 3\}; v \in \{0, 1, 2\}; w \in \{0, 1\} \}$

4. $\omega \cap div\ 2.268 = \{ 2^u \cdot 3^v \cdot 7^w \mid \ldots \}$

5. $\omega \cap div\ \{1.400, 2.268\} = \{ 2^u \cdot 7^v \mid u \in \{0, 1, 2\}; v \in \{0, 1\} \}$

6. $1.400 \wedge 2.268 = 2^2 \cdot 3^0 \cdot 5^0 \cdot 7^1$

7. Calcula $\omega \cap div\ a$

Ahora es fácil calcular el m.a.c.d. y el m.b.c.m. de toda cupla de naturales, de los cuales se conocen las factorizaciones primas.

PROPOSICION 2

Si $b = p_1^{b_1} p_2^{b_2} \ldots p_k^{b_k}$ y $c = p_1^{c_1} p_2^{c_2} \ldots p_k^{c_k}$

donde los p_i son naturales primos distintos dos a dos
los b_i y los c_i son naturales,

Entonces $b \wedge c = p_1^{g_1} p_2^{g_2} \ldots p_k^{g_k}$ y $b \vee c = p_1^{m_1} p_2^{m_2} \ldots p_k^{m_k}$

donde para todo $i \in \{1, \ldots, k\}$:
g_i es el menor y m_i es el mayor de los números b_i, c_i

PROPOSICION 3

El producto de toda cupla de naturales es igual al producto de su m.a.c.d. por su m.b.c.m.

Es decir,

Para todo $b, c \in \omega$: $\boxed{b\,c = b \wedge c \cdot b \wedge c}$

DEMOSTRACION :

El lector verificará sin dificultad que la proposición es válida cuando uno de los números b o c es igual a 0 ó a 1

Luego, supongamos b y c distintos de 0 y de 1

Con las anotaciones de la proposición 2

$$b \cdot c = p_1^{b_1+c_1} p_2^{b_2+c_2} \ldots p_k^{b_k+c_k}$$

$$b \wedge c \cdot b \vee c = p_1^{g_1+m_1} p_2^{g_2+m_2} \ldots p_k^{g_k+m_k}$$

Pero, para todo $i \in \{1, \ldots, k\}$: $b_i + c_i = g_i + m_i$

l. q. q. d.

Si los naturales b, c no son nulos,

Entonces $b \wedge c \neq 0$ y la fórmula de la proposición 3 se escribe

$$\boxed{b \vee c = \frac{b\,c}{b \wedge c}}$$

EJERCICIOS

1. Para todo $a, b \in \mathbf{Z}$: $\quad a \wedge b \cdot a \vee b = |a\ b|$

2. Si $\quad a \in \omega \quad$ y $\quad b \in \omega_0$

Entonces $\quad \dfrac{a}{a \wedge b} = \dfrac{a \vee b}{b}$

3. *Calcula*

$36 \vee 25$, $42 \vee 112$, $512 \vee 336$, $12.024 \vee 4.645$

PROPOSICION 4 — Para todo $a, b, c \in \mathbf{Z}$:

$$a \wedge c = 1 \implies a \wedge b = a \wedge bc$$

DEMOSTRACION :

Basta establecer la proposición cuando a, b, c son naturales.

Dejamos al lector la verificación en el caso en que los números a, b, c son 0 ó 1.

En adelante supondremos que $a, b, c \in \omega \setminus \{0, 1\}$

Con anotaciones evidentes, y los p_i designando números primos distintos dos a dos, se tiene

$$a = {p_1}^{a_1} \cdot {p_2}^{a_2} \cdot \ldots \cdot {p_n}^{a_n}$$

$$b = {p_1}^{b_1} \cdot {p_2}^{b_2} \cdot \ldots \cdot {p_n}^{b_n} \cdot p_*^* \cdot p_*^* \cdot \ldots \cdot p_*^*$$

$$c = p_*^* \cdot p_*^* \cdot \ldots \cdot p_*^* \qquad \text{(puesto que } a \wedge c = 1\text{)}$$

$$bc = {p_1}^{b_1} \cdot {p_2}^{b_2} \cdot \ldots \cdot {p_n}^{b_n} \cdot p_*^* \cdot p_*^* \cdot \ldots \cdot p_*^*$$

Luego en virtud de la proposición 2

$$a \wedge b = {p_1}^{g_1} \cdot \ldots \cdot {p_n}^{g_n} = a \wedge bc$$

de donde

$\forall i \in \{1, \ldots, n\}$: $\quad g_i$ es el menor de los naturales a_i , b_i

l. q. q. d.

2 – NUMEROS NATURALES PRIMARIOS

DEFINICION

Se llaman **números (naturales) primarios** *a las potencias* $\mathbf{p}^n$
donde **p** *es un natural* **primo** *y* **n** *es un número natural* **no nulo**
$\mathbf{p}^n$ *es el natural primario de número* **primo p** *y* **de exponente n**

He aquí un fragmento del cuadro (infinito) de naturales primarios.

				.	.						
.	.	.	.	.	.	.					
.	.	.	.	.	.	.	.	.			
.	.	.	.	11^9	13^9	.	.	.	.		
2^8	3^8	5^8	7^8	11^8	13^8	17^8	.	23^8	.	.	
2^7	3^7	5^7	7^7	11^7	13^7	17^7	19^7	23^7	.	.	
2^6	3^6	5^6	7^6	11^6	13^6	17^6	19^6	23^6	29^6	.	
2^5	3^5	5^5	7^5	11^5	13^5	17^5	19^5	23^5	29^5	31^5	...
2^4	3^4	5^4	7^4	11^4	13^4	17^4	19^4	23^4	29^4	31^4	...
2^3	3^3	5^3	7^3	11^3	13^3	17^3	19^3	23^3	29^3	31^3	...
2^2	3^2	5^2	7^2	11^2	13^2	17^2	19^2	23^2	29^2	31^2	...
2	3	5	7	11	13	17	19	23	29	31	...

CUADRO DE LOS NUMEROS NATURALES PRIMARIOS

FIG. 40

A menudo será cómodo representar los naturales primarios mediante puntos dispuestos de la siguiente manera :

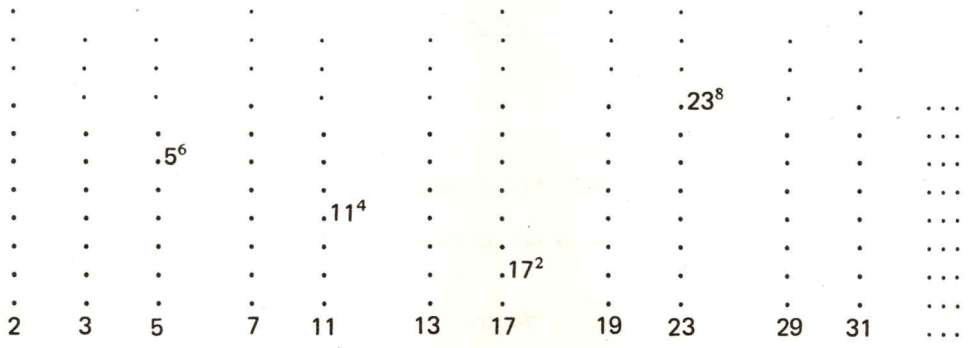


DIAGRAMA DE LOS NUMEROS NATURALES PRIMARIOS

FIG. 41

EJEMPLOS

1. El conjunto de números naturales primarios es numerable.

2. Los naturales 0 y 1 no **son primarios.**

3. Los números 6, 10, 100, 1.964, no son **primarios.**

4. Todos los naturales primos son primarios.

5. Todo natural estrictamente mayor que 1 es un producto de naturales primarios cuyos números primos son distintos dos a dos.

DEFINICION

Para todo $n \in \omega$, se anota $q(n)$ el conjunto de divisores naturales primarios de n

EJEMPLOS Y PROPIEDADES INMEDIATAS

1. $$18 = 2 \cdot 3^2 \quad ; \quad 720 = 2^4\ 3^2\ 5$$

$$q\,(18) = \{2, 3, 3^2\} \quad ; \quad q\,(720) = \{2, 2^2, 2^3, 2^4, 3, 3^2, 5\}$$

2. $$q\,(1) = \phi$$

3. $q\,(0)$ = conjunto de naturales primarios

   $q\,(0)$ es un conjunto infinito.

4. Para todo $n \in \omega$: $q(n) \subset div\ (n)$

   Para todo $n \in \omega_0$: $div\ (n)$ es un conjunto finito.

   Para todo $n \in \omega_0$: $q(n)$ es un conjunto finito.

5. **Si** $n \in \omega$

Entonces $q(n)$ es infinito $\iff$ $n = 0$

6. En virtud de la prop. 6 del c. 4 :

$\forall\, n \in \omega \setminus \{1\}$: $q(n) \neq \phi$

7. **Si** $n \in \omega$

Entonces $q(n) = \phi \iff n = 1$

8. Cuáles son los más altos divisores naturales primarios de

$$720 = 2^4 \cdot 3^2 \cdot 5^1$$

9. **Si** n es un natural estrictamente mayor que 1

Entonces n es el producto de sus más altos divisores naturales primarios.

10. **Si** conoces $q(n)$ (finito y no vacío)

Entonces conoces los más altos divisores naturales primarios de n

Luego, conoces n

11.

Si $a, b \in \omega$

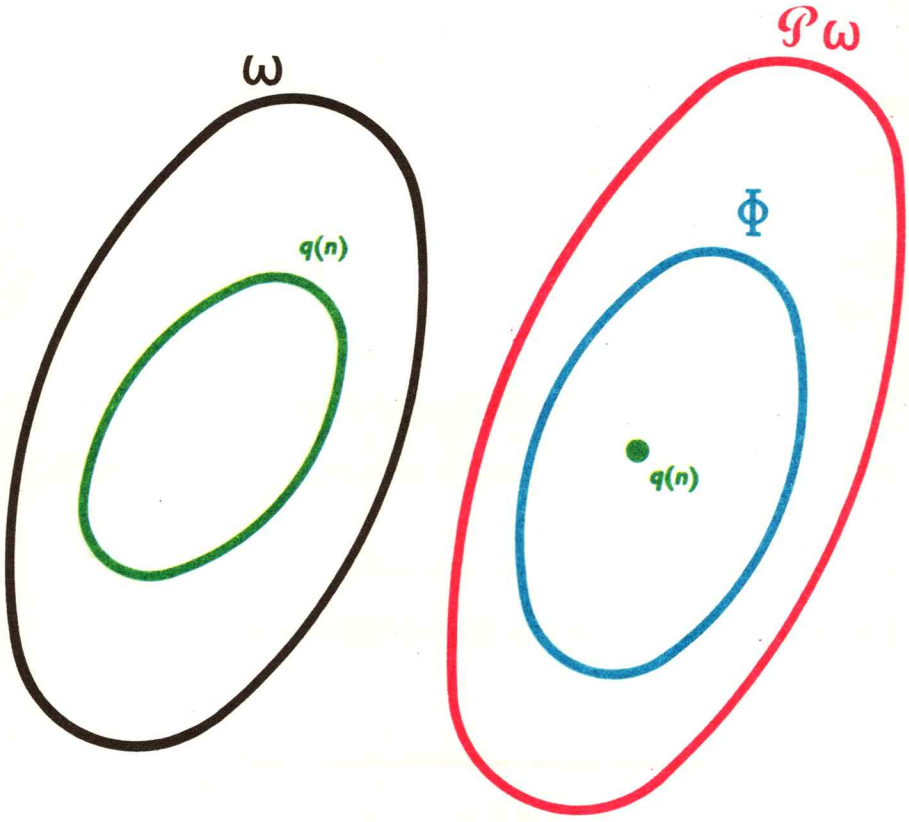
Entonces $q(a) = q(b) \iff a = b$

DEFINICION

$$\Phi = \{ q(n) \mid n \in \omega \}$$

Si $n \in \omega$

Entonces



$q(n) \subset \omega$

$q(n) \in \Phi \subset \mathscr{P}\omega$

FIG. 42

Tengamos en cuenta que Φ es **conjunto de partes** de $q(0)$

$\phi = q(1) \in \Phi$ y $q(0)$ es el único conjunto infinito perteneciente a Φ

Hemos demostrado la

PROPOSICION 5

$q : \omega \to \Phi : n \to q(n)$ *es una* **biyección.**

Luego, para todo $a, b \in \omega$: $q(a) = q(b) \iff a = b$

Además $q(a) = \phi \iff a = 1$

$q(a)$ es infinito $\iff a = 0$

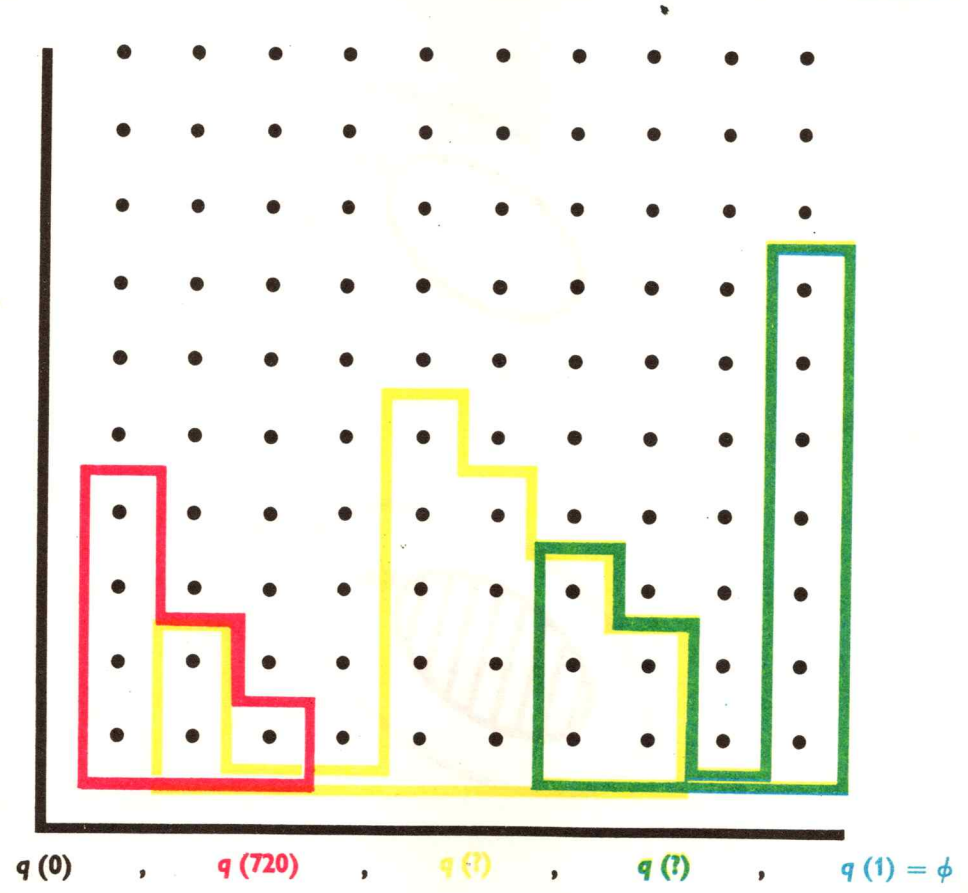


FIG. 43

EJERCICIOS

1.

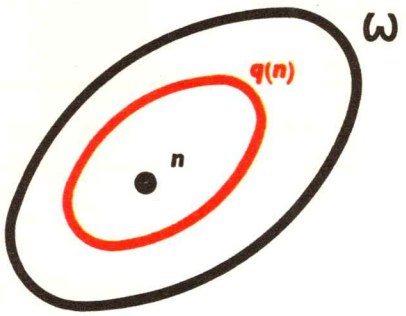


FIG. 44

¿Qué sabes de n?

2.

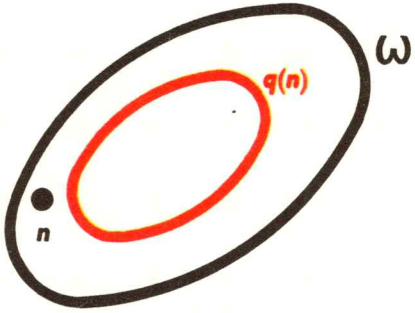


FIG. 45

¿Qué sabes de n?

3.

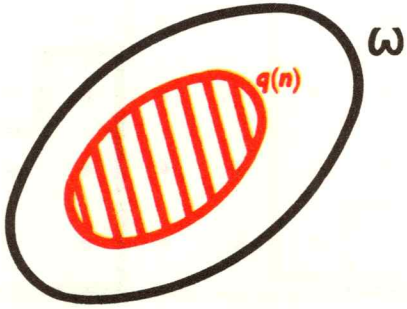
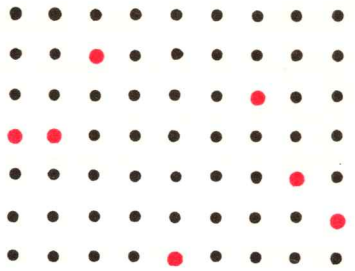


FIG. 46

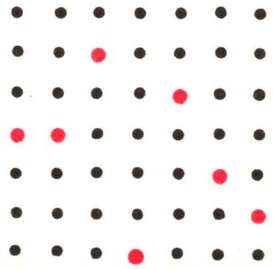
¿Qué sabes de n?

3 – ISOMORFISMO $\mathfrak{q} : \omega, | \rightarrow \Phi, \subset$

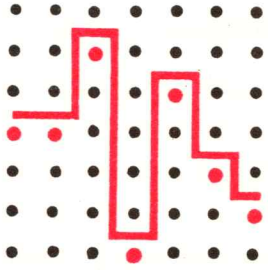
En el diagrama de los números naturales primarios, marca con rojo un número finito de primarios cuyos números primos son distintos dos a dos.



Dejando de lado las columnas en las cuales no figura ningún punto rojo, se obtiene este esquema.



El natural *a*, producto de estos números primarios, queda perfectamente representado por esta escalera.



Dibuja un diagrama de Venn del conjunto $q(a)$

$(\# q(a) = 25)$

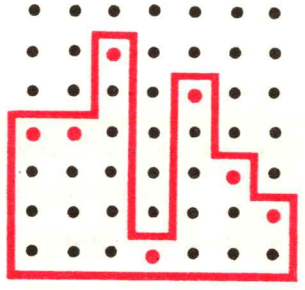
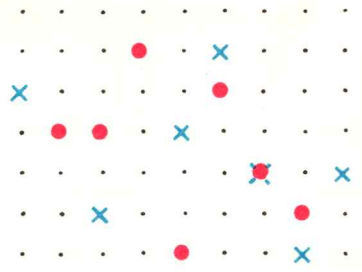
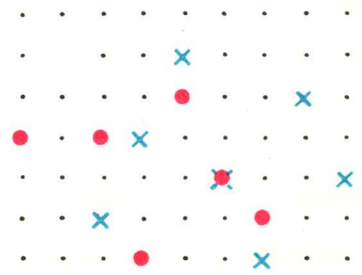


FIG. 47

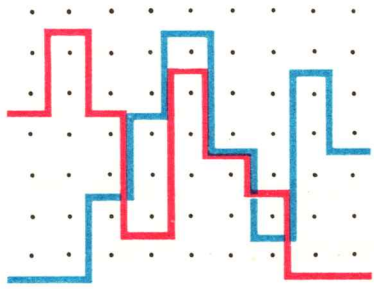
Piensa en dos números naturales $a, b > 1$
En el diagrama de naturales primarios, representa los más altos divisores naturales primarios de a con puntos rojos, y los de b con cruces azules.
(Deja de lado las columnas vacías).



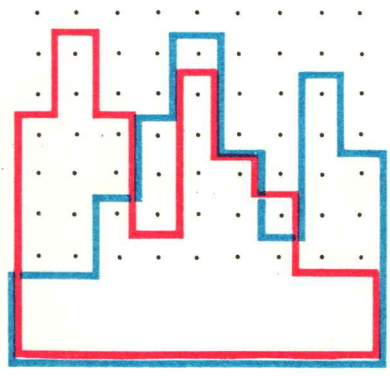
Permutando eventualmente las columnas, se obtiene este esquema, más claro.



Los naturales a y b o sus más altos divisores naturales primarios están perfectamente representados por estas escaleras.



Dibuja diagramas de Venn de los conjuntos $q(a)$ y $q(b)$



Cada vez que a y b designen naturales > 1, supondremos las escaleras trazadas como acabamos de indicar.

FIG. 48

He aquí los naturales $a, b > 1$

En virtud de la proposición 1

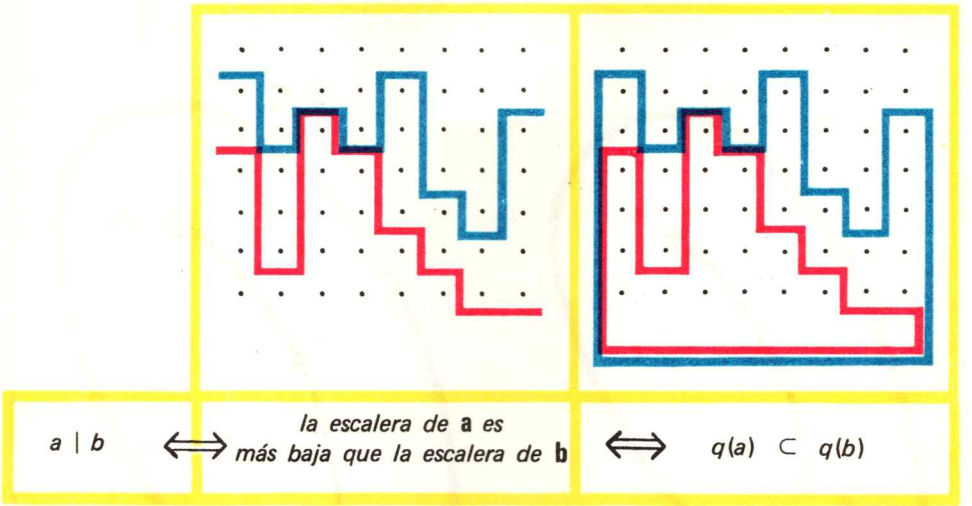


FIG. 49

PROPOSICION 6

Para todo $a, b \in \omega$: $\quad a \mid b \iff q(a) \subset q(b)$

DEMOSTRACION :

Ya hemos probado esta equivalencia cuando los naturales a, b son estrictamente mayores que 1

1 es el elemento más bajo de $\omega, |$
$q(1)$ es el menor elemento de $\Phi, \subset$

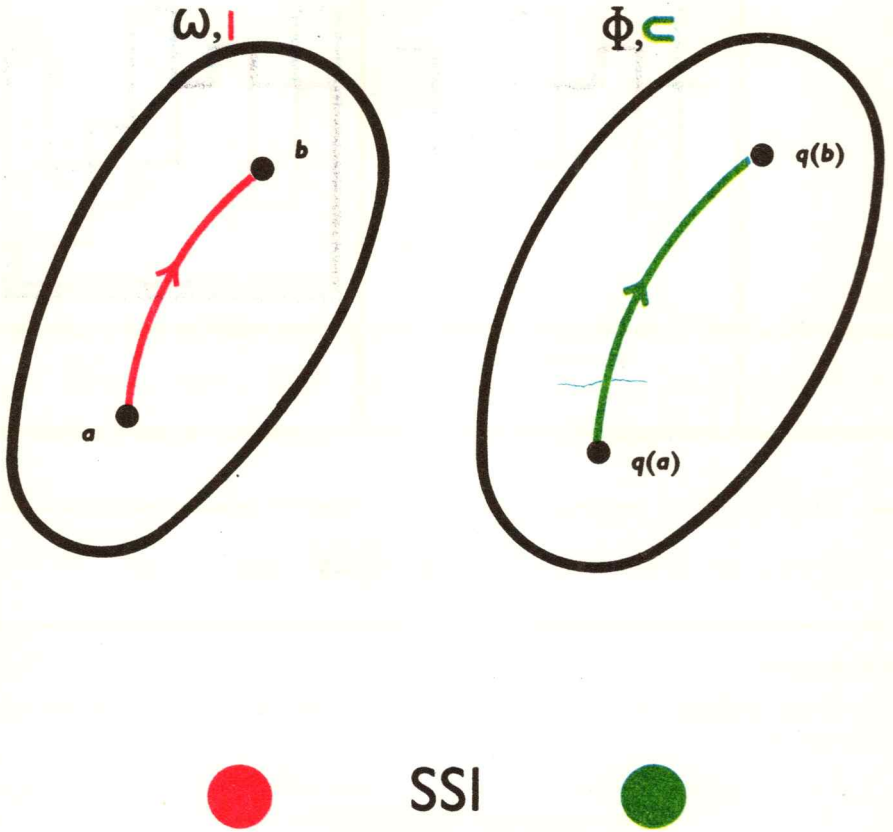
0 es el elemento más alto de $\omega, |$
$q(0)$ es el mayor elemento de $\Phi, \subset$

La equivalencia $\quad a \mid b \iff q\,(a) \subset q\,(b)$

es, pues, verdadera para todo $a, b \in \omega$

l. q. q. d.

PROPOSICION 5-6



$q : \omega \rightarrow \Phi : n \rightarrow q(n)$

ES UN **ISOMORFISMO** DEL CONJUNTO ORDENADO ω, $|$

SOBRE EL CONJUNTO ORDENADO Φ, $\subset$

FIG. 50

4 – ISOMORFISMO q : ω, Λ, V, | → Φ, ∩, ∪, ⊂

He aquí los naturales $a, b > 1$

En virtud de la proposición 2 :

La escalera de $a \wedge b$
es la más alta de las escaleras que
son más bajas que las de a y de b

Dibuja en verde la escalera de $a \wedge b$

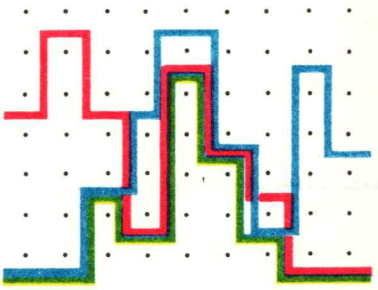


FIG. 51

Dibuja diagramas de Venn de $q(a)$, $q(b)$ y $q(a \wedge b)$

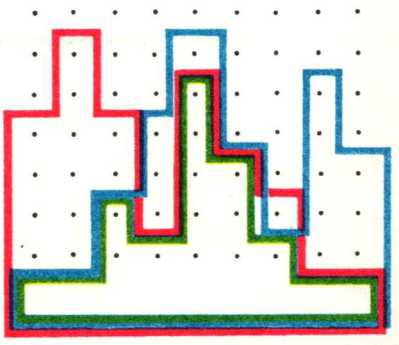


FIG. 53

La escalera de $a \vee b$
es la más baja de las escaleras que
son más altas que las de a y de b

Dibuja en amarillo la escalera de $a \vee b$

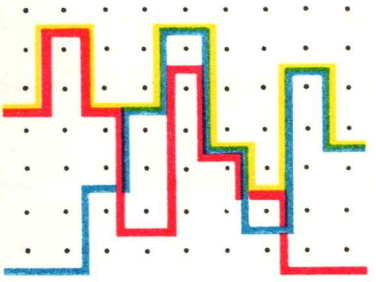


FIG. 52

Dibuja diagramas de Venn de $q(a)$, $q(b)$ y $q(a \vee b)$

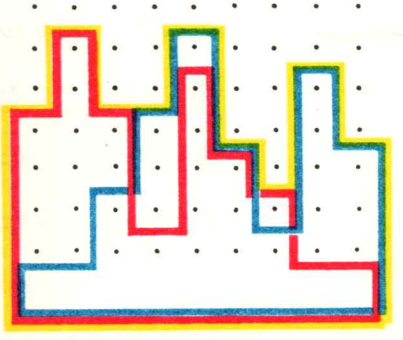


FIG. 54

¿Qué hemos probado?

Si a, b son naturales > 1

Entonces $q(a \wedge b) = q(a) \cap q(b)$; $q(a \vee b) = q(a) \cup q(b)$

El lector verificará sin dificultad que estas fórmulas continúan siendo válidas cuando por lo menos uno de los números $a, b \in \{0, 1\}$

De donde resulta la

PROPOSICION 7

Para todo **a, b** $\in \omega$: $q(a \wedge b) = q(a) \cap q(b)$; $q(a \vee b) = q(a) \cup q(b)$

Las proposiciones 5, 6 y 7 se expresan simultáneamente en el

TEOREMA 1

$$q : \omega \to \Phi : n \to q(n)$$

es un isomorfismo de $\omega, \wedge, \vee, |$ **sobre** $\Phi, \cap, \cup, \subset$

"CASO PARTICULAR" DEL **TEOREMA DE STONE**

En fórmulas :

Para todo a, b $\in \omega$:

$$q(a) = q(b) \iff a = b$$

$$q(a) \text{ infinito} \iff a = 0$$

$$q(a) = \phi \iff a = 1$$

$$a \mid b \iff q(a) \subset q(b)$$

$$q(a \wedge b) = q(a) \cap q(b) \quad ; \quad q(a \vee b) = q(a) \cup q(b)$$

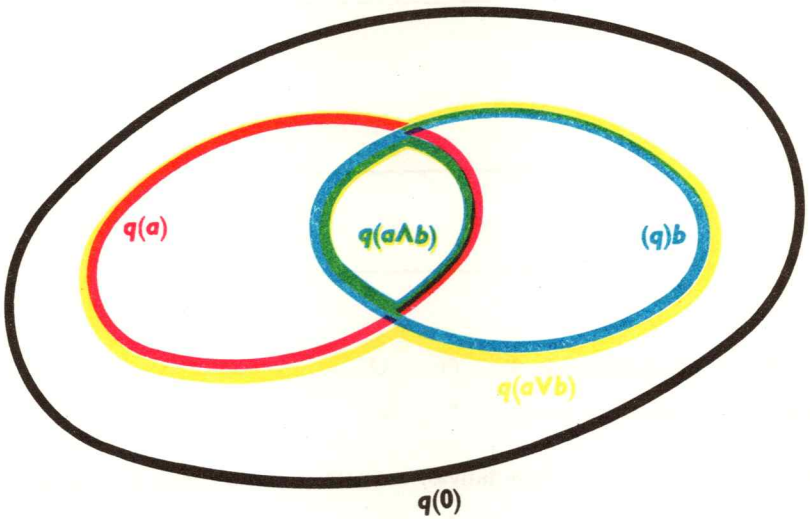


FIG. 55

5 – PROPIEDADES DE ω, ∧, ∨

Como q^{-1} : $\Phi \rightarrow \omega$: $q(n) \rightarrow n$

es un isomorfismo de $\Phi, \cap, \cup$ sobre $\omega, \wedge, \vee$ |

las propiedades de $\Phi, \cap, \cup$ se transmiten a $\omega, \wedge, \vee$

$$\Phi \ , \ \cap \ , \ \cup$$

es un modelo perfecto de

$$\omega \ , \ \wedge \ , \ \vee$$

Todas las propiedades de Φ , $\cap$, $\cup$
se reflejan perfectamente en ω , $\wedge$, $\vee$

Las leyes $\cap$ y $\cup$ son conmutativas, asociativas y mutuamente distributivas.

Luego

Las leyes $\wedge$ y $\vee$ son conmutativas, asociativas y mutuamente distributivas.

TEOREMA 2

En ω, ∧, ∨ las leyes ∧ y ∨ son conmutativas, asociativas y mutuamente distributivas.

0 es neutro para ∧ y absorbente para ∨

1 es neutro para ∨ y absorbente para ∧

Como consecuencia de la asociatividad de $\wedge$ y $\vee$ escribiremos, como de costumbre :

Para todo $a, b, c \in \omega$: $a \wedge b \wedge c = (a \wedge b) \wedge c = a \wedge (b \wedge c)$

$a \vee b \vee c = (a \vee b) \vee c = a \vee (b \vee c)$

Además, en virtud de la asociatividad general (MM2, c. 7, § 6),

para todo $a_1, \ldots, a_k \in \omega$: $a_1 \wedge \ldots \wedge a_k$ y $b_1 \vee \ldots \vee b_k$ designan números naturales bien determinados.

$a_1 \wedge \ldots \wedge a_k$ es el más alto de los divisores naturales de $\{ a_1, \ldots a_k \}$

Luego $a_1 \wedge \ldots \wedge a_k = \wedge \{ a_1, \ldots, a_k \}$

Análogamente $a_1 \vee \ldots \vee a_k$ es el más bajo de los múltiplos naturales de todos los a_i , lo que nos permite anotar

$$a_1 \vee \ldots \vee a_k = \vee \{ a_1, \ldots, a_k \}$$

Definimos el m.a.c.d. $\wedge P$ de toda parte P de **Z** y el m.b.c.m. $\vee P$ de toda parte finita P de **Z**

Si P es una parte infinita de ω

Entonces ¿cuál es el conjunto de números naturales que son múltiplos de todos los elementos de P?

En virtud del teorema de la factorización prima de los naturales, es fácil ver que este conjunto es $\{ 0 \}$

Así resulta que el m.b.c.m. de toda parte infinita de ω es 0

Si P es una parte infinita de ω

Entonces $\vee P = 0$

EJERCICIOS

1. ω es el conjunto de múltiplos naturales de todos los elementos de ϕ

2. $$\vee \phi \quad = 1$$

3. $$\vee \{0\} = 0$$

4. $\wedge$ y $\vee$ definen leyes internas en **Z**

   Estas leyes son asociativas, conmutativas y mutuamente distributivas.

5. Para todo $a, b, c \in \omega_0$:

$$a \vee b \vee c = \frac{a\,b\,c \cdot a \wedge b \wedge c}{a \wedge b \cdot a \wedge c \cdot b \wedge c}$$

$$= \frac{abc}{ab \wedge ac \wedge bc}$$

6. Para todo $a, b, c, d \in \omega_0$:

$$a \vee b \vee c \vee d = \frac{abcd}{abc \wedge abd \wedge acd \wedge bcd}$$

7. Para todo $a_1, \ldots, a_n \in \omega_0$:

$$a_1 \vee a_2 \vee \ldots \vee a_n = \frac{a_1 \cdot \ldots \cdot a_n}{a_1 \ldots a_{n-1} \wedge a_1 \ldots a_{n-2}\, a_n \wedge \ldots \wedge a_2 \ldots a_n}$$

MARSHALL STONE

Es un matemático americano nacido en Nueva York en 1903.

Realizó sus estudios en la famosa Universidad de Harvard, donde obtuvo su título de doctor (Ph. D.) en 1926, después de haber trabajado en su especialidad, durante un año, en la Universidad de París. Fue profesor en las Universidades de Harvard, Columbia, Yale y se radicó en Chicago desde 1946 (ha sido Director del Departamento de Matemática, desde 1946 hasta 1952).

Su obra científica abarca los dominios más variados de la matemática, desde las teorías próximas a la lógica hasta el estudio de los fundamentos de la física cuántica.

Estudió mucho los espacios de HILBERT – tan importantes en física – que son espacios vectoriales que no admiten ninguna base finita, pero que sin embargo están provistos de un producto escalar estrictamente positivo, como el vectorial euclídeo plano introducido en [MM3].

En el capítulo 9 del primer libro verás que toda transformación de un cuerpo finito K es una función polinomio

$$K \to K : x \quad k_n x^n + \ldots + k_1 x + k_0$$

donde $n \in \omega$ y los $k_i \in K$

No sucede lo mismo con el cuerpo de números reales. El matemático alemán WEIERSTRASZ mostró que sin embargo se pueden aproximar las transformaciones continuas definidas en ciertas partes de R por las funciones polinomio. Marshall STONE llegó a generalizar considerablemente este teorema.

El teorema de STONE que citamos en este libro, fue establecido en 1934 entre otros resultados importantes referentes a reticulados.

STONE recibió, gracias a sus trabajos, importantes distinciones científicas. Es miembro de la Academia de Ciencias de los Estados Unidos y de varias academias extranjeras. Es doctor honoris causa de muchas Universidades.

Desde la Antigüedad, casi todos los matemáticos han sido intrépidos viajeros. Marshall STONE es fiel a esta tradición y recorre incansablemente el globo terrestre para exponer en todas partes el fruto de sus investigaciones y meditaciones.

En el curso de los últimos años, este gran matemático se interesó en el problema de la enseñanza de la matemática en todos los niveles y contribuyó enormemente a impulsar el actual movimiento de modernización.

En 1959 presidió el histórico Congreso de ROYAMONT donde el matemático francés Jean DIEUDONNE lanzó el famoso anatema

"¡ABAJO EUCLIDES!"

1 – RETICULADOS

DEFINICION

El conjunto ordenado E, $\leqslant$ es un RETICULADO

ssi

Para todo $a, b \in E$:

el conjunto G de elementos de E mayores que a y b comprende un elemento menor que todo elemento de G

Este elemento necesariamente único se anota $a \vee b$

y

Para todo $a, b \in E$:

el conjunto P de elementos de E menores que a y b comprende un elemento mayor que todo elemento de P

Este elemento necesariamente único se anota $a \wedge b$

EJEMPLOS

1. El conjunto $\mathcal{P}$ E, $\subset$ de partes de E (ordenado por la inclusión) es un reticulado para el cual
$$\wedge = \cap \quad \text{y} \quad \vee = \cup$$

2. ω, | es un reticulado.

3. Todo conjunto totalmente ordenado es un reticulado.

   En este caso, $a \wedge b = min \{ a, b \}$ y $a \vee b = max \{ a, b \}$

4. El conjunto de convexos de Π, ordenado por la inclusión, es un reticulado.
Se observará que $\wedge = \cap$ y $\vee \neq \cup$

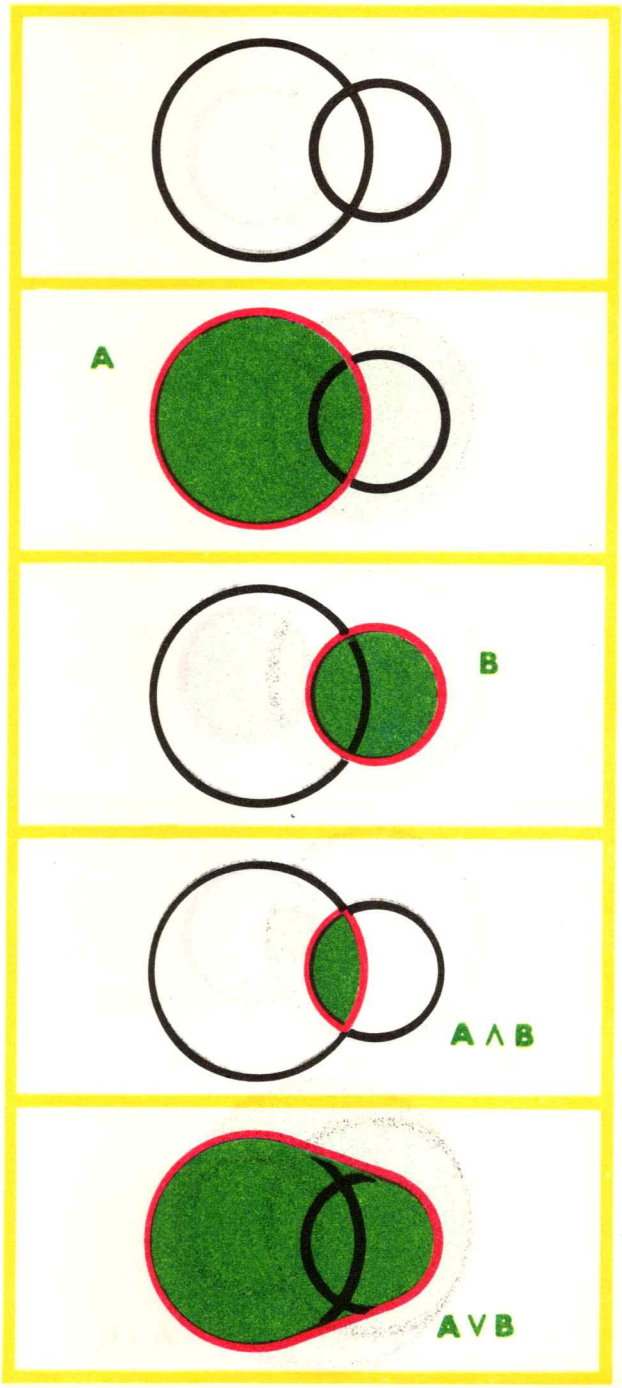


FIG. 56

EN EL RETICULADO
DE CONVEXOS DEL PLANO

5. El conjunto de círculos abiertos de Π, ordenado por la inclusión, es un reticulado. Se observará que $\wedge \neq \cap$ y $\vee \neq \cup$

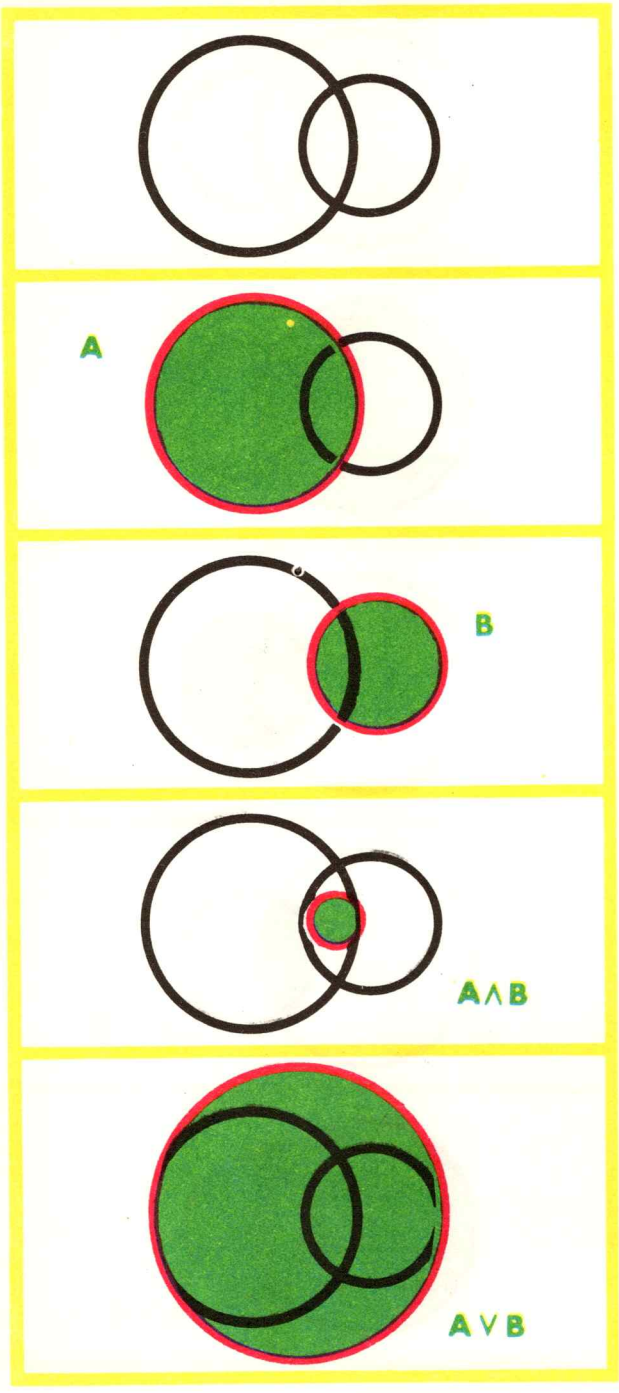


FIG. 57

EN EL RETICULADO
DE CIRCULOS ABIERTOS

6. Es fácil construir conjuntos ordenados que no sean reticulados. Por ejemplo, considerando partes propias de ciertos reticulados.

7. $(\mathcal{P}E \setminus \{\phi\}), \subset$ no es un reticulado.

8. $(\mathcal{P}E \setminus \{E\}), \subset$ no es un reticulado.

9. $(\omega \setminus \{1\}), \mid$ no es un reticulado.

10. El conjunto S de subgrupos de Z, + es un reticulado para el cual $\wedge = \cap$ y $\vee = +$

11. El conjunto de sub-vectoriales de un espacio vectorial es un reticulado para el cual $\wedge = \ldots$ y $\vee = \ldots$

En todo reticulado T, $\leqslant$

las leyes internas totalmente definidas $\wedge$ *y* $\vee$

son

asociativas, conmutativas, idempotentes

Es decir,

Si *a, b, c* designan elementos del reticulado T, $\leqslant, \wedge, \vee$

Entonces

$(a \wedge b) \wedge c = a \wedge (b \wedge c)$ *(asociatividad)*

$a \wedge b = b \wedge a$ *(conmutatividad)*

$a \wedge a = a$ *(idempotencia)*

2 – RETICULADOS DISTRIBUTIVOS

DEFINICION

el reticulado T, $\leqslant, \wedge, \vee$ **es distributivo**

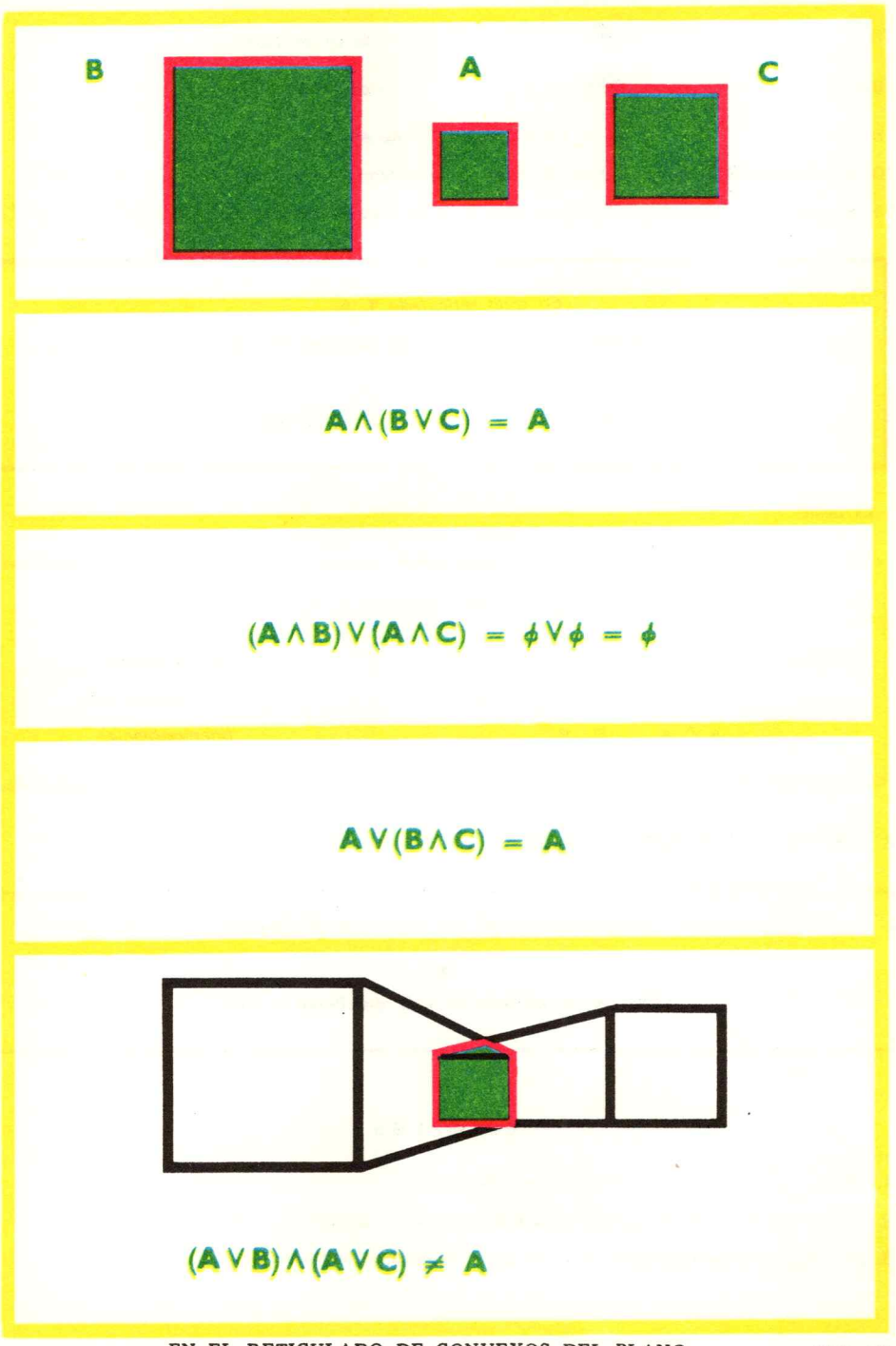
ssi

cada una de las leyes $\wedge$ *y* $\vee$ **distribuye** *la otra*

EJEMPLOS

1. $\mathcal{P}E., \subset, \cap, \cup$ es un reticulado distributivo.
2. Ya demostramos en el capítulo 6 que el reticulado $\omega, \mid, \wedge, \vee,$ es distributivo.
3. El conjunto S de subgrupos de Z, + es un reticulado distributivo.

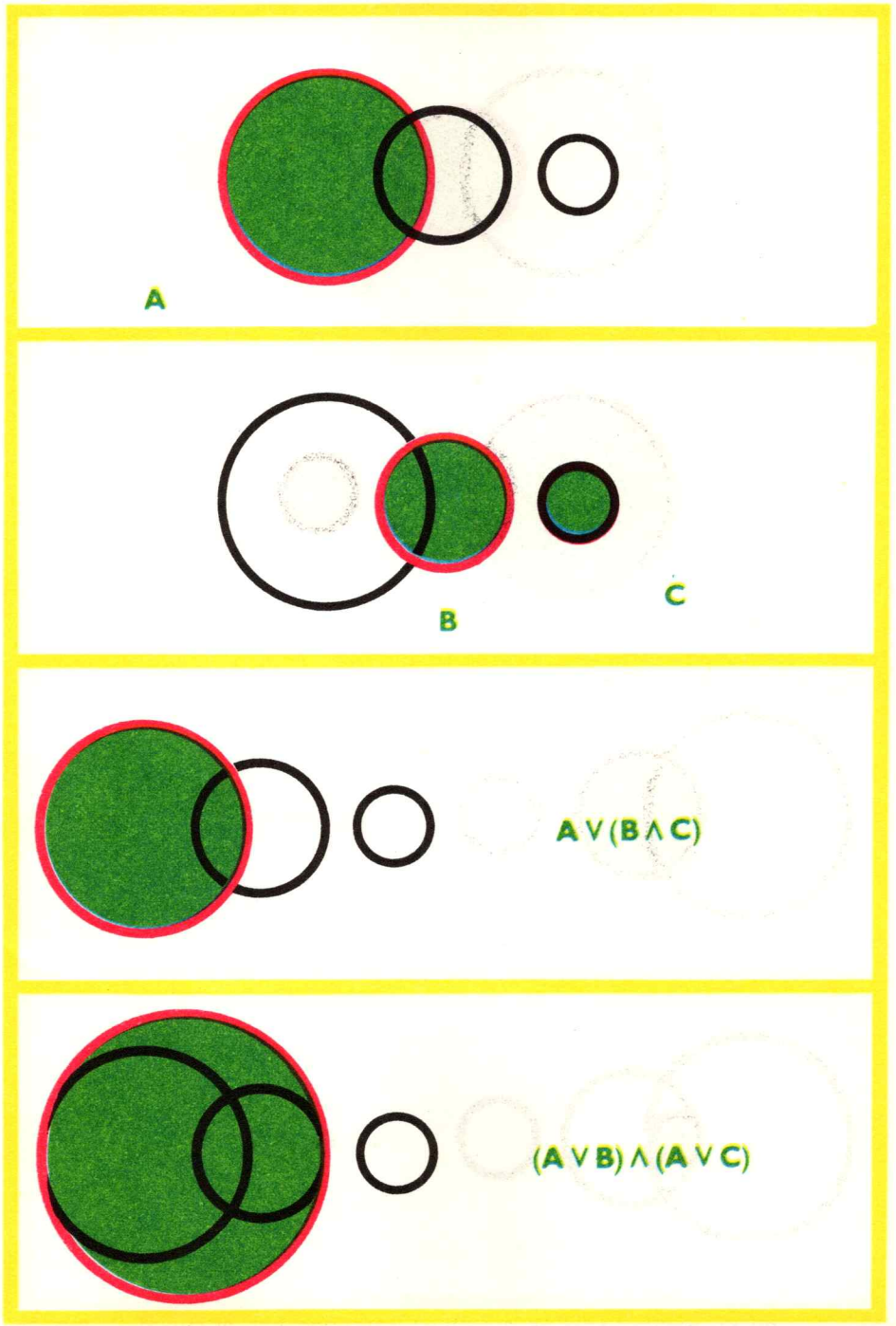
4. El reticulado de conjuntos convexos del plano no es distributivo.



EN EL RETICULADO DE CONVEXOS DEL PLANO

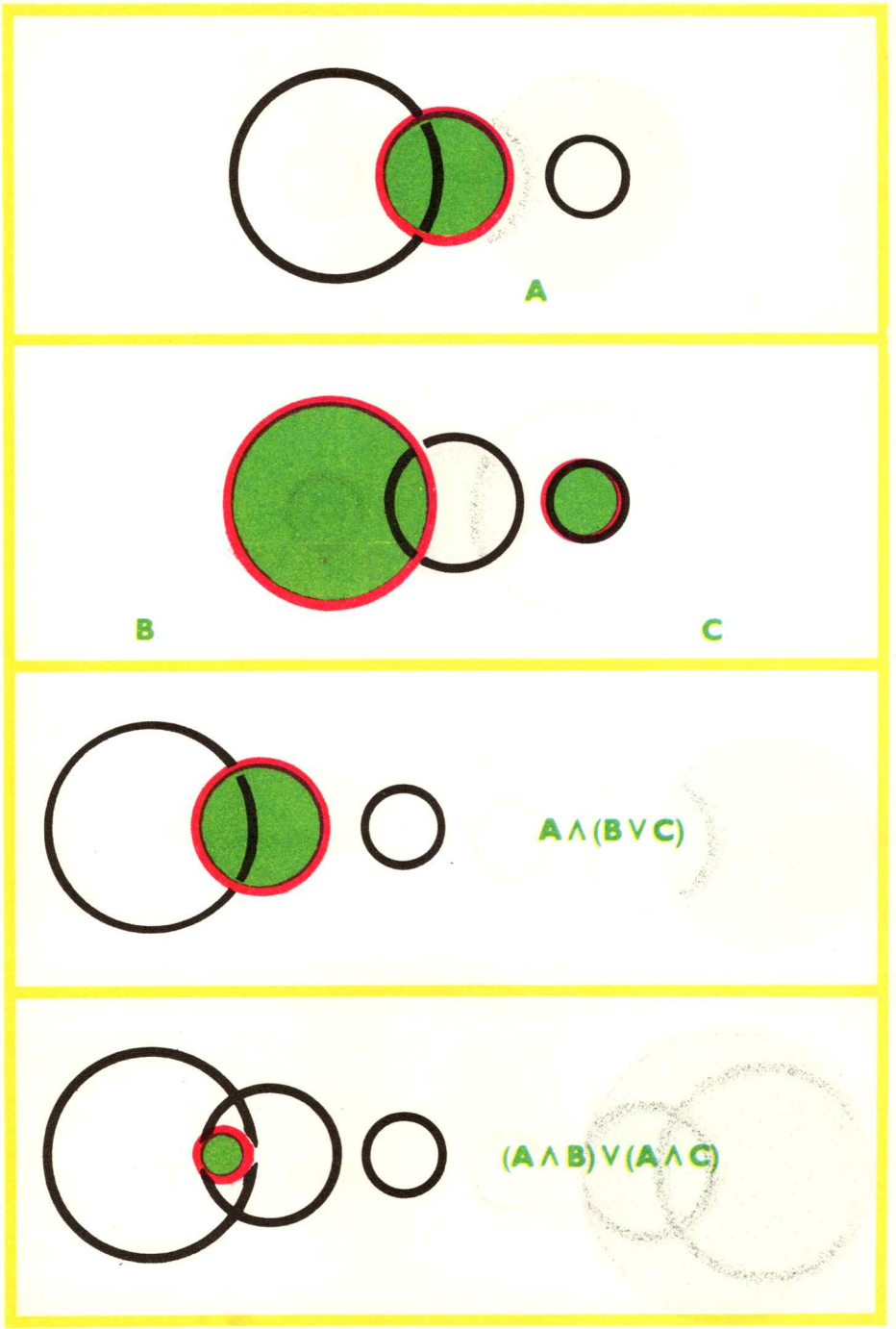
FIG. 58

5. El reticulado de Círculos abiertos del plano no es distributivo.



EN EL RETICULADO DE CIRCULOS ABIERTOS DEL PLANO II FIG. 59

El reticulado de círculos abiertos del plano no es distributivo.



EN EL RETICULADO DE CIRCULOS ABIERTOS DEL PLANO Π FIG. 60

EJERCICIOS

1. Explica los . . . "necesariamente único" . . . de la definición de reticulados.

2. Las leyes de todo reticulado son conmutativas.

3. El conjunto $\mathcal{C}$ de círculos cerrados del plano (conjunto ordenado por la inclusión) no es un reticulado.

   El conjunto ordenado $\mathcal{C} \cup \{\phi\}$ es un reticulado.

3 – TEOREMA DE STONE (1934)

Todo reticulado distributivo complementado es isomorfo a un reticulado $\mathcal{P}, \subset, \cap, \cup$ donde $\mathcal{P}$ es un conjunto de conjuntos.

Un reticulado $T, \leqslant, \wedge, \vee$ se llama *complementado*

ssi

T admite el mínimo Δ, el máximo ∇

y

$$\forall\, t \in T\,,\ \exists\, t' \in T : \quad t \vee t' = \nabla \text{ y } t \wedge t' = \Delta$$

No demostraremos aquí el teorema de STONE.

Hemos establecido la distributividad del reticulado $\omega, |, \wedge, \vee$ exhibiendo un isomorfismo con el reticulado $\Phi, \subset, \cap, \cup$ lo cual está de acuerdo con el espíritu del teorema de STONE.

LIBRO 3

LA ARITMETICA DE LOS NUMEROS RACIONALES

6

La Aritmética de los Números racionales

1 — NUMEROS RACIONALES

$$\mathbb{Q} = \{ a/b \mid a \in \mathbb{Z},\ b \in \omega_0 \}$$

$$\mathbb{Q}^+ = \{ q \in \mathbb{Q} \mid q \geqslant 0 \}$$

$$\mathbb{Q}_0 = \{ q \in \mathbb{Q} \mid q \neq 0 \}$$

$$\mathbb{Q}_0^+ = \{ q \in \mathbb{Q} \mid q > 0 \}$$

$\mathbb{Q}$ es el conjunto de (números) **racionales.**

$\mathbb{Q}^+$ es el conjunto de racionales **positivos.**

$\mathbb{Q}_0$ es el conjunto de racionales **no nulos.**

$\mathbb{Q}_0^+$ es el conjunto de racionales **positivos no nulos,**
es decir, de racionales **estrictamente positivos.**

$$\omega \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$$

EJERCICIOS

1. Q , $+$ es un grupo conmutativo cuyo elemento neutro es 0

2. Q_0 , $\cdot$ es un grupo conmutativo, cuyo elemento neutro es 1

3. Q , $+$, $\cdot$ es un subcuerpo de **R**

4. Q_0^+ , $\cdot$ es un grupo conmutativo.

5. Q^+ , Q^- , Q_0^+ , Q_0^- son partes de Q estables para la adición, que no son subgrupos de Q , $+$

6. El conjunto B de números binarios limitados es un subanillo de Q, +, · pero no es un subcuerpo de Q , $+$, $\cdot$

7. El conjunto L de números decimales limitados es . . .

8. Q , $+$, $\cdot$, $\leqslant$ es un subcuerpo ordenado de R

9. Q , $+$, $\cdot$, $\leqslant$ es un cuerpo arquimedeano.

10. Q , $+$, $\cdot$, $\leqslant$ no satisface el axioma de continuidad.

2 – FRACCIONES PARCIALES

PROPOSICION 1

Si $a \in \mathbf{Z}$; $b, c \in \mathbf{Z}_0$; $b \wedge c = 1$

Entonces $\dfrac{a}{b\,c} = \dfrac{z_1}{b} + \dfrac{z_2}{c}$ con $z_1, z_2 \in \mathbf{Z}$

DEMOSTRACION :

Como $b \wedge c = 1$, existen enteros racionales b', c' tales que

$$b'\,b + c'\,c = 1$$

Por lo tanto

$$\frac{a}{b\,c} = \frac{a \cdot 1}{b\,c} = \frac{a\,(b'\,b + c'\,c)}{b\,c}$$

$$= \frac{a\,b'\,b}{b\,c} + \frac{a\,c'\,c}{b\,c}$$

$$= \frac{a\,b'}{c} + \frac{a\,c'}{b}$$

l. q. q. d.

Todo número racional $q \in \mathbf{Q}$ se escribe

$$q = \frac{a}{d} \qquad \text{con } a \in \mathbf{Z} \quad \text{y} \quad d \in \omega_0$$

Si $d > 1$ **Entonces** d se escribe $d = {p_1}^{d_1} \cdot \ldots \cdot {p_n}^{d_n}$

(teorema de la factorización prima de los números naturales).

donde los p_i son números naturales primos distintos dos a dos
y los d_i son naturales no nulos.

PROPOSICION 2

Si $a \in \mathbf{Z}$ *y* $p_1, \ldots, p_n$ *son números primos distintos dos a dos*

y $d_1, \ldots, d_n$ *son naturales no nulos*

Entonces

$$\frac{a}{{p_1}^{d_1} \cdot \ldots \cdot {p_n}^{d_n}} = \frac{a_1}{{p_1}^{d_1}} + \frac{a_2}{{p_2}^{d_2}} + \ldots + \frac{a_n}{{p_n}^{d_n}}$$

con $a_1, \ldots, a_n \in \mathbf{Z}$

DEMOSTRACION :

En virtud de la proposición 1 se tiene, sucesivamente

$$\frac{a}{{p_1}^{d_1} \cdot \ldots \cdot {p_n}^{d_n}} = \frac{a_1^1}{{p_1}^{d_1}} + \frac{b_2}{{p_2}^{d_2} \cdot \ldots \cdot {p_n}^{d_n}}$$

(con $a_1, b_2 \in \mathbf{Z}$) (puesto que ${p_1}^{d_1} \wedge {p_2}^{d_2} \ldots {p_n}^{d_n} = 1$)

$$= \frac{a_1}{{p_1}^{d_1}} + \frac{a_2}{{p_2}^{d_2}} + \frac{b_3}{{p_3}^{d_3} \cdot \ldots \cdot {p_n}^{d_n}}$$

(con $a_2, b_3 \in \mathbf{Z}$) (puesto que ${p_2}^{d_2} \wedge {p_3}^{d_3} \ldots {p_n}^{d_n} = 1$)

$$= \frac{a_1}{{p_1}^{d_1}} + \frac{a_2}{{p_2}^{d_2}} + \ldots + \frac{a_n}{{p_n}^{d_n}}$$

(con $a_1, \ldots, a_n \in \mathbf{Z}$)

l. q. q. d.

PROPOSICION 3

Si $a \in \mathbf{Z}$, $b \in \omega_0$, $n \in \omega_0$

Entonces

$$\frac{a}{b^n} = z + \frac{r_1}{b} + \frac{r_2}{b_2} + \ldots + \frac{r_n}{b^n}$$

donde $z, r_1, \ldots, r_n$ *son enteros racionales tales que*

Para todo $i \in \{ 1, \ldots, n \} : \quad 0 \leqslant r_i \leqslant b$

DEMOSTRACION :

Efectuaremos n divisores euclídeas por b

Todas las letras designan enteros racionales
y para todo $i \in \{1, \ldots, n\}$: $0 \leqslant r_i < b$

$$
\begin{aligned}
q_n &= q_{n-1}\, b + r_{n-1} \\
q_{n-1} &= q_{n-2}\, b + r_{n-2} \\
&\vdots \\
q_3 &= q_2\, b + r_2 \\
q_2 &= z\, b + r_1
\end{aligned}
\qquad
\begin{aligned}
a &= q_n\, b + r_n \\
&= (q_{n-1}\, b + r_{n-1})\, b + r_n \\
&= q_{n-1}\, b^2 + r_{n-1}\, b + r_n \\
&= (q_{n-2}\, b + r_{n-2})\, b^2 + r_{n-1}\, b + r_n \\
&= q_{n-2}\, b^3 + r_{n-2}\, b^2 + r_{n-1}\, b + r_n \\
&\vdots \\
&= q_2\, b^{n-1} + r_2\, b^{n-2} + \ldots + r_{n-1}\, b + r_n \\
&= z\, b^n + r_1\, b^{n-1} + r_2\, b^{n-2} + \ldots + r_{n-1}\, b + r_n \\
\frac{a}{b^n} &= z + \frac{r_1}{b} + \frac{r_2}{b^2} + \ldots + \frac{r_{n-1}}{b^{n-1}} + \frac{r_n}{b^n}
\end{aligned}
$$

l. q. q. d.

DEFINICION

Se llaman **fracciones parciales** *a los racionales*

$$\frac{r}{p^n} \quad \textit{donde} \quad n \in \omega_0 \;,\; p \textit{ es un número natural primo}$$

y r *es un natural tal que* $0 \leqslant r < p$

p^n *es el denominador de la fracción parcial* r/p^n

TEOREMA 1

Todo racional es la suma de un entero racional y de fracciones parciales (cuyos denominadores son distintos dos a dos).

DEMOSTRAC'ON :

El teorema resulta trivial para los racionales enteros.

Todo racional no entero q se escribe $q = a/b$ con $a \in \mathbf{Z}$ y $1 < b \in \omega$

Luego

$$q = \frac{a}{p_1^{d_1} \cdot \ldots \cdot p_n^{d_n}}$$ (en virtud del teorema de la factorización prima de los naturales)

$$= \frac{a_1}{p_1^{d_1}} + \ldots + \frac{a_n}{p_n^{d_n}} \quad \text{con } a_1 \ldots, a_n \in \mathbf{Z}$$ (en virtud de la proposicion 2)

Ahora bien, en virtud de la proposición 3, cada uno de los $\dfrac{a_i}{p_i^{d_i}}$ es la suma de un entero racional y de fracciones parciales.

l. q. q. d.

3 – LA RELACION ... DIVIDE ... DEFINIDA EN Q

$\mathbf{Q}$, + es un grupo conmutativo.

$\mathbf{Z}$ es un subgrupo de $\mathbf{Q}$, +

He aquí un racional q

– ¿Cuál es el subgrupo de $\mathbf{Q}$, + engendrado por q?

– es decir, el menor subgrupo de $\mathbf{Q}$, + que comprende q

– El subgrupo de $\mathbf{Q}$, + engendrado por q es

$$\{\ldots, -3q, -2q, (-1)q = -q, 0 = 0q, q = 1q, 2q, 3q, 4q, \ldots\}$$

– Anotaremos muy naturalmente este grupo

$$q\mathbf{Z} = \{qz \mid z \in \mathbf{Z}\}$$

Diremos además que $q\mathbf{Z}$ es el conjunto de **múltiplos** de q

DEFINICION

Para todo $a, b \in \mathbf{Q}$: $a \mid b \iff$ *existe* $z \in \mathbf{Z}$ *tal que* $b = zq$

La expresión *"a | b"* se lee *"a* **divide** *b"*

Como antes, también se expresa $a \mid b$ diciendo que

"a es un divisor de b" o **"b es múltiplo de a"**

"a es más bajo que b" o **"b es más alto que a"**

$$\forall\, a, b \in \mathbf{Q}: \quad a \mid b \iff b \in a\mathbf{Z} = \mathbf{Z}a$$

La relación | así definida en $\mathbf{Q}$ **prolonga** la relación | ya definida en $\mathbf{Z}$

EJERCICIOS

1. $\frac{2}{3} \nmid \frac{4}{7}$; $\frac{1}{4} \mid \frac{1}{2}$; $\frac{5}{8} \mid 0$; $\frac{2}{3} \mid 2$

   $\frac{12}{49} \nmid \frac{131}{7}$; $1 \nmid \frac{1}{2}$; $\frac{12}{49} \mid \frac{48}{7}$

2. **Si** $q_1 \in \mathbf{Q}_0$, $q_2 \in \mathbf{Q}$

   Entonces $q_1 \mid q_2 \iff \frac{q_2}{q_1} \in \mathbf{Z}$

3. **Si** $a, b, c, d \in \mathbf{Z}_0$

   Entonces $\frac{a}{b} \mid \frac{c}{d} \iff ad \mid bc$

4. Para todo $q_1, q_2 \in \mathbf{Q}$: $(q_1 \mid q_2 \text{ y } q_2 \mid q_1) \iff q_1 = \pm q_2$

5. La relación $\mid$ definida en **Q** es reflexiva y transitiva.
   Pero no es ni simétrica ni antisimétrica.

6. **Si** $q_1, q_2 \in \mathbf{Q}^+$
   Entonces $(q_1 \mid q_2 \text{ y } q_2 \mid q_1) \iff q_1 = q_2$

7. $\mathbf{Q}^+$, $\mid$ es un conjunto ordenado no total.

8. El número 0 es el más alto elemento de **Q** , $\mid$

9. **Q** , $\mid$ no comprende ningún elemento más bajo que todo elemento de **Q**

10. $\mathbf{Q}^+$, $\mid$ no comprende un elemento más bajo.

11. **Si** $\mathrm{P} \subset \mathbf{Q}$ **Entonces** $div\ \mathrm{P} = \{ q \in \mathbf{Q} \mid \forall p \in \mathrm{P} : q \mid p \}$

    Si $\mathrm{B} = \{ \frac{1}{2^n} \mid n \in \omega \}$ **Entonces** $div\ \mathrm{B} = \phi$

    Los elementos de B no admiten ningún divisor común.

4 – FACTORIZACIONES PRIMAS DE LOS NUMEROS RACIONALES

Demostraremos que todo número racional q distinto de $0, 1, -1$ admite una única **factorización prima**

$$q = \pm {p_1}^{q_1} \ldots {p_n}^{q_n}$$

donde los p_i son naturales primos distintos dos a dos
y los q_i son **enteros racionales**, no todos nulos.

El signo $+$ se utiliza, evidentemente, para los racionales estrictamente positivos, el signo $-$ para los racionales estrictamente negativos.

Por lo tanto, podemos limitarnos a considerar sólo el caso de racionales estrictamente positivos, distintos de 1

Para establecer la unicidad de las factorizaciones primas en ω, utilizamos el hecho de que

Si $p_1, \ldots, p_n$ son naturales primos distintos dos a dos
y $a_1, \ldots, a_n$ son naturales, no todos nulos,

Entonces ${p_1}^{a_1} \ldots {p_n}^{a_n} \neq 1$

Comencemos por demostrar una proposición análoga cuando los exponentes son enteros racionales.

PROPOSICION 4

Si $p_1 \ldots p_n$ *son naturales primos distintos dos a dos,*
y $a_1 \ldots a_n$ **son enteros racionales,**

Entonces ${p_1}^{a_1} \ldots {p_n}^{a_n} = 1 \Longleftrightarrow$ *todos los* a_i *son nulos.*

La implicación $\Longleftarrow$ es evidente.

DEMOSTRACION DE $\Longrightarrow$

$$p_1^{a_1} \ldots p_n^{a_n} = \frac{p_1^{b_1} \ldots p_n^{b_n}}{p_1^{c_1} \ldots p_n^{c_n}} = 1$$

donde $\forall i \in \{1, \ldots, n\}$: b_i es el mayor y $-c_i$ es el menor de los números 0, a_i

$$p_1^{b_1} \ldots p_n^{b_n} = p_1^{c_1} \ldots p_n^{c_n} \qquad (1)$$

Para todo $i \in \{1, \ldots, n\}$, uno de los números b_i, c_i, es nulo y el otro es igual a $|a_i|$

Siendo naturales los exponentes que figuran en la fórmula (1), aplicamos el teorema de la factorización prima de los números naturales,

$$\forall i \in \{1, \ldots, n\} \quad : \quad b_i = c_i \ldots = 0$$

$$\forall i \in \{1, \ldots, n\} \quad : \quad a_i = 0$$

l. q. q. d.

TEOREMA 2

Todo racional q distinto de 0, 1, −1

admite una sola factorización prima

$$q = \pm p_1^{q_1} \ldots p_h^{q_h}$$

donde los p_i son naturales primos distintos dos a dos y los q_i son enteros racionales no nulos.

TEOREMA DE LA FACTORIZACION PRIMA DE NUMEROS RACIONALES

DEMOSTRACION :

1º Existencia

He aquí $q \in \mathbb{Q}_0^+$ y $q \neq 1$

$$q = \frac{a}{b} \qquad \text{con} \qquad a, b \in \omega_0$$

En virtud del teorema de la factorización prima de números naturales, y gracias al subterfugio de los exponentes nulos,

$$q = \frac{{p_1}^{a_1} \ldots {p_n}^{a_n}}{{p_1}^{b_1} \ldots {p_n}^{b_n}}$$

donde los p_i son naturales primos distintos dos a dos y los a_i, b_i son naturales.

Luego $$q = {p_1}^{a_1 - b_1} \ldots {p_n}^{a_n - b_n}$$

Como $q \neq 1$, los $a_i - b_i$ no son todos nulos.

Dejemos de lado los ${p_i}^{a_i - b_i}$ para los cuales $a_i - b_i = 0$

Mediante una eventual nueva numeración de los p restantes, se obtiene finalmente

$$q = {p_1}^{q_1} \ldots {p_h}^{q_h}$$

donde los p_i son naturales primos distintos dos a dos
y los q_i son enteros racionales, no todos nulos.

2º Unicidad

He aquí naturales primos distintos dos a dos $p_1 \ldots p_n$
y enteros racionales $a_1 \ldots a_n, b_1 \ldots b_n$

Si $${p_1}^{a_1} \ldots {p_n}^{a_n} = {p_1}^{b_1} \ldots {p_n}^{b_n}$$

Entonces

$$\frac{{p_1}^{a_1} \ldots {p_n}^{a_n}}{{p_1}^{b_1} \ldots {p_n}^{b_n}} = 1$$

$${p_1}^{a_1 - b_1} \ldots {p_n}^{a_n - b_n} = 1$$

$$a_1 - b_1 = \ldots = a_n - b_n = 0 \qquad \text{(prop. 4)}$$

l. q. q. d.

He aquí $z \in \mathbf{Z}_0$ y $q \in \mathbf{Q}_0$

$$z = \pm {p_1}^{n_1} \ldots {p_k}^{n_k} \qquad q = \pm {p_1}^{q_1} \ldots {p_k}^{q_k}$$

donde los p_i son naturales primos distintos dos a dos
los n_i son naturales
los q_i son enteros racionales

$$z \cdot q = \pm {p_1}^{n_1+q_1} \ldots p^{n_k+q_k}$$

De donde resulta la

PROPOSICION 5

Si $a = \pm {p_1}^{a_1} \ldots {p_n}^{a_n}$, $b = \pm {p_1}^{b_1} \ldots {p_n}^{b_n}$

donde los p_i son naturales primos distintos dos a dos y los a_i, b_i son enteros racionales,

Entonces $a \mid b \iff \forall i \in \{1, \ldots, n\} : a_i \leqslant b_i$

Luego, resulta que

La relación | definida en $\mathbf{Q}$ *es reflexiva y transitiva.*

Además, $\forall a, b \in \mathbf{Q} : (a \mid b \text{ y } b \mid a) \iff a = \pm b$

En particular,

Si $a, b \in \mathbf{Q}^+$ **Entonces** $(a \mid b \text{ y } b \mid a) \iff a = b$

$\mathbf{Q}^+$, | *es un conjunto ordenado pero no totalmente*

EJERCICIOS

1. $\frac{1}{6} = 2^{-1} \cdot 3^{-1}$ $\qquad$ $\frac{12}{49} = 2^2 \cdot 3 \cdot 7^{-2}$

$\frac{7}{2} = 7 \cdot 2^{-1}$ $\qquad$ $0{,}625 = 2^{-3} \cdot 5$

$0{,}002 = 2^{-2} \cdot 5^{-3}$

2. Dibuja el esquema de la relación | en el conjunto

$$\left\{ \frac{2}{5} \; ; \; 0{,}25 \; ; \; 1 \; ; \; -0{,}25 \; ; \; \overline{\frac{15}{28}} \; ; \; \frac{1}{3} \; ; \; 0 \right\}$$

5 – M.A.C.D. Y M.B.C.M. DE CUPLAS DE NUMEROS RACIONALES

Consideremos primero el caso en el cual uno de los racionales es nulo.

Todo racional divide 0 y 0 es el único múltiplo de 0

Para todo $q \in \mathbf{Q}$, el número $|q|$ es el único racional positivo cuyo conjunto de divisores igual al conjunto de divisores comunes de 0 y q

Este hecho se expresa diciendo que $|q|$ es el m.a.c.d. de 0 y de q
lo cual se anota

$$0 \wedge q = |q| = q \wedge 0$$

0 es el único número racional múltiplo común de 0 y q

Este hecho se expresa diciendo que 0 es el m.b.c.m. de 0 y q,
lo cual se anota

$$0 \vee q = 0 = q \vee 0$$

He aquí los racionales no nulos $a = \pm {p_1}^{a_1} \ldots {p_n}^{a_n}$, $b = \pm {p_1}^{b_1} \ldots {p_n}^{b_n}$

donde los p_i son naturales primos distintos dos a dos y los a_i , b_i son enteros racionales.

Para todo i, designaremos con g_i el menor y con m_i el mayor de los enteros racionales a_i , b_i

En virtud de la proposición 5, el número $g = {p_1}^{g_1} \ldots {p_n}^{g_n}$ es el único racional positivo cuyo conjunto de divisores es el conjunto de divisores comunes a a y b

Este hecho se expresa diciendo que g es el m.a.c.d. de los racionales a, b, y se anota

$$a \wedge b = g = b \wedge a$$

Análogamente, $m = {p_1}^{m_1} \ldots {p_n}^{m_n}$ es el único racional positivo cuyo conjunto de múltiplos es el conjunto de múltiplos comunes de a y b

Este hecho se expresa diciendo que m es el m.b.c.m. de los racionales a y b y se anota

$$a \vee b = m = b \vee a$$

PROPOSICION 6

Si $a = \pm {p_1}^{a_1} \dots {p_n}^{a_n}$ y $b = \pm {p_1}^{b_1} \cdot \dots \cdot {p_n}^{b_n}$

donde los p_i *designan números naturales primos distintos dos a dos y los* $a_i, b_i \in \mathbf{Z}$

Entonces

$$a \wedge b = {p_1}^{g_1} \cdot \dots \cdot {p_n}^{g_n} \quad \text{y} \quad a \vee b = {p_1}^{m_1} \cdot \dots \cdot {p_n}^{m_n}$$

donde para todo i : g_i *es el menor y* m_i *es el mayor de los números* a_i, b_i

Además, para todo $q \in \mathbf{Q}$: $0 \wedge q = |q| = q \wedge 0$ y $0 \vee q = 0 = q \vee 0$

Estas fórmulas muestran que las leyes $\wedge$, $\vee$ definidas en $\mathbf{Q}$ prolongan las anteriormente definidas en $\mathbf{Z}$

Además

$\forall a, b \in \mathbf{Q}$: $\quad a \wedge b \cdot a \vee b = |a \cdot b|$

$\forall a, b, c \in \mathbf{Q}$: $\quad ac \wedge bc = |c| \cdot a \wedge b$ y $ac \vee bc = |c| \cdot a \vee b$

En particular

$$\forall a, b \in \mathbf{Z};\ \forall n \in \omega_0 : \quad \frac{a}{n} \wedge \frac{b}{n} = \frac{a \wedge b}{n} \quad \text{y} \quad \frac{a}{n} \vee \frac{d}{n} = \frac{a \vee b}{n}$$

Pero toda cupla de racionales se escribe $\frac{a}{n}, \frac{b}{n}$ con $a, b \in \mathbf{Z}$ y $n \in \omega_0$

Luego

Para todo $a, b, c \in \mathbf{Q}$:

$a \wedge b$	$= b \wedge a$	$a \vee b$	$= b \vee a$
$a \wedge (b \wedge c)$	$= (a \wedge b) \wedge c$	$a \vee (b \vee c)$	$= (a \vee b)\ H\ c$
$a \wedge (b \vee c)$	$= (a \wedge b) \vee (a \wedge c)$	$a \vee (b \wedge c)$	$= (a \vee b) \wedge (a \vee c)$

PROPOSICION 7 — *En* $\mathbf{Q}$, $\wedge$, $\vee$

Las leyes $\wedge$, $\vee$ *son conmutativas, asociativas y mutuamente distributivas.*

Evidentemente, sucede lo mismo en $\mathbf{Q}^+$, $\wedge$, $\vee$

Se observará que en $\mathbf{Q}^+$, $\wedge$, $\vee$: 0 es neutro para $\wedge$ y absorbente para $\vee$
la ley $\vee$ no admite neutro
la ley $\wedge$ no admite absorbente.

PROPOSICION 7 — *En* $\mathbf{Q}$:

El m.a.c.d. de toda cupla de racionales es combinación lineal con coeficientes enteros racionales de las componentes de la cupla.

DEMOSTRACION :

He aquí $q_1, q_2 \in \mathbf{Q}$

Sean $q_1 = a/n$ y $q_2 = b/n$ con $a, b \in \mathbf{Z}$ y $n \in \omega_0$

Luego

$$q_1 \wedge q_2 = \frac{a}{n} \wedge \frac{b}{n} = \frac{a \wedge b}{n}$$

Ahora bien $a \wedge b = a'a + b'b$ con $a', b' \in \mathbf{Z}$

De donde

$$q_1 \wedge q_2 = \frac{a \wedge b}{n} = \frac{a'a + b'b}{n} = a' \cdot \frac{a}{n} + b' \cdot \frac{b}{n} = a'q_1 + b'q_2$$

l.q.q.d

Como consecuencia de la asociatividad de $\wedge$, el m.a.c.d. $q_1 \wedge \ldots \wedge q_n$ de toda sucesión de racionales queda claramente definido.

Aplicando la proposición 8, resulta fácilmente que

$$q_1 \wedge \ldots \wedge q_n = z_1 q_1 + \ldots + z_n q_n \quad \text{donde los} \quad z_i \in \mathbf{Z}$$

EJERCICIOS

1. $\forall\, a, b \in \mathbf{Q}$: $a \wedge b = (-a) \wedge b = a \wedge (-b) = (-a) \wedge (-b) = |a| \wedge |b|$

$a \vee b = (-a) \vee b = a \vee (-b) = (-a) \vee (-b) = |a| \vee |b|$

2. $\frac{1}{2} \vee \frac{1}{3} =$; $\boxed{\frac{2}{3} \wedge 1 = \frac{1}{3}}$; $\frac{1}{2} \wedge \frac{1}{3} =$; $\frac{1}{2} \wedge \frac{2}{3} =$

$\frac{1}{2} \vee \frac{2}{3} =$; $\frac{4}{7} \vee \frac{5}{2} =$; $\frac{4}{7} \wedge \frac{5}{2} =$; $2 \wedge \frac{1}{2} =$

$0{,}25 \wedge 625 =$; $\frac{7}{4} \wedge \frac{2}{5} =$; $\boxed{\frac{2}{3} \vee 1 = 2}$; $0{,}003 \wedge 7{,}2 =$

3. $\forall\, a, b \in \mathbf{Q}$: $a \wedge b = 1 \iff a, b \in \mathbf{Z}$

4. $\forall\, a, b \in \mathbf{Q}_0$: $a^{-1} \vee b^{-1} = (a \wedge b)^{-1}$; $a^{-1} \wedge b^{-1} = (a \vee b)^{-1}$

5. $\forall\, q \in \mathbf{Q}_0$: $q \vee q^{-1} = (q \wedge q^{-1})^{-1}$

6. $\forall\, a, b \in \mathbf{Q}_0^+$: $a \vee b = (a \wedge b)^{-1} \iff b = a^{-1}$

7. Toda cupla de números racionales primos entre sí
es una cupla de números enteros racionales primos entre sí.

8. $\forall a, b \in \mathbf{Q}$: $a \wedge b \in \omega \iff a, b \in \omega$

9. $\forall\, a, b, c, d \in \omega_0$:

$a \wedge b = 1$ y $c \wedge d = 1$ $\Longrightarrow \frac{a}{b} \wedge \frac{c}{d} = \frac{a \wedge c}{b \vee d}$

$\Longrightarrow \frac{a}{b} \vee \frac{c}{d} = \frac{a \vee c}{b \wedge d}$

10. El número 1 es absorbente de ω , $\wedge$ y neutro de ω , $\vee$

El número 1 no es absorbente de $\mathbf{Q}$, $\wedge$ ni neutro de $\mathbf{Q}$, $\vee$

6 – SUBGRUPOS DE $\mathbf{Q}$, +

He aquí $a, b \in \mathbf{Q}$

Ya sabemos que el menor subgrupo de $\mathbf{Q}$, + que comprende a es

$$mod\ a = a\mathbf{Z} = \{ za \mid z \in \mathbf{Z} \}$$

El menor subgrupo de $\mathbf{Q}$, + que contiene $\{a, b\}$ es

$$mod\ \{a, b\} = \{ a'a + b'b \mid a', b' \in \mathbf{Z} \}$$

PROPOSICION 9

$\forall\, a, b \in \mathbf{Q}$: $\qquad mod\ \{a, b\} = mod\ (a \wedge b)$

DEMOSTRACION :

1) $a \wedge b = a'a + b'b$ con $a', b' \in \mathbf{Z}$ (prop. 8)

$a \wedge b \in mod\ \{a, b\}$

$mod\ \{a, b\}$ es **un** subgrupo de $\mathbf{Q}$, + que comprende $a \wedge b$

$mod\ (a \wedge b)$ es **el menor** subgrupo de $\mathbf{Q}$, + que comprende $a \wedge b$

$$\boxed{mod\ (a \wedge b) \subset mod\ \{a, b\}}$$

2) $(a \wedge b) \mid a$ luego $a \in mod\ (a \wedge b)$

$(a \wedge b) \mid b$ luego $b \in mod\ (a \wedge b)$

$mod\ (a \wedge b)$ es **un** subgrupo de $\mathbf{Q}$, + que contiene $\{a, b\}$

$mod\ \{a, b\}$ es **el menor** subgrupo de $\mathbf{Q}$, + que contiene $\{a, b\}$

$$\boxed{mod\ \{a, b\} \subset mod\ (a \wedge b)}$$

I. q. q. d.

Generalizando, para toda parte finita $F = \{q_1, \ldots, q_n\} \subset Q$ el menor subgrupo de **Q** , + que contiene F es

$$mod\ F = \{z_1\ q_1 + \ldots + z_n\ q_n \mid z_1, \ldots, z_n \in \mathbf{Z}\}$$

De la observación final del § 4 también se tiene que

$$mod\ \{q_1, \ldots, q_n\} = mod\ (q_1 \wedge \ldots \wedge q_n)$$

De manera que *todo subgrupo de* **Q** , + *engendrado por una parte finita de* **Q** , + *está engendrado por uno de sus elementos.*

Pero no sucede lo mismo con todos los subgrupos de **Q** , +

El conjunto L de decimales limitados es un subgrupo de **Q** , +

Este subgrupo no está engendrado por ninguno de sus elementos.

En efecto, sea *b* un número decimal limitado que tiene exactamente *n* cifras después de la coma.

Los elementos de *mod b* son, por consiguiente, decimales limitados que comprenden, *a lo sumo n* cifras después de la coma.

Luego 0, 0 . . . 0 1 pertenece a L pero no pertenece a *mod b*

($n + 1$ cifras)

l. q. q. d.

EJERCICIOS

1. El conjunto de binarios limitados es un subgrupo de **Q**, + que no está engendrado por ninguno de sus elementos.

2. **Q** es un subgrupo de **Q**, + que no está engendrado por ninguno de sus elementos.

3. Justifica cada etapa de la demostración de la proposición 9.

LIBRO 4

ANILLOS CONMUTATIVOS
Y
CUERPOS

7

Anillos y cuerpos residuales o de restos

1 — EL ANILLO Z_n , + , ·

He aquí un número $n > 1$

Sea $Z_n = \{0, 1, 2, \ldots, n-2, n-1\}$

Para todo $z \in \mathbf{Z}$, designemos mediante $\overline{z}$ el **resto** de la división euclídea de z por n

$$\forall z \in \mathbf{Z}: \quad z = qn + \overline{z} \quad \text{con} \quad q \in \mathbf{Z} \quad \text{y} \quad 0 \leqslant \overline{z} < n$$

De este modo queda definida la **suryección**

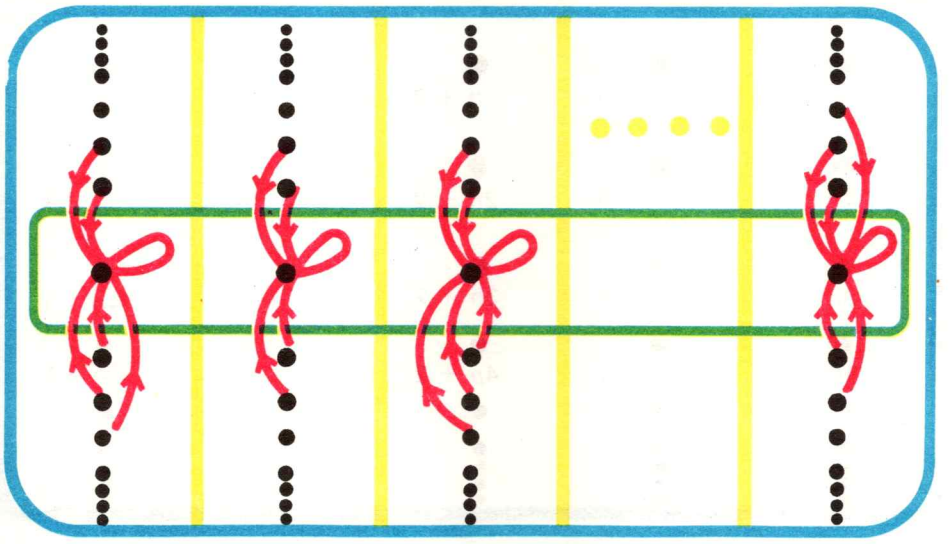


FIG. 61

RESTO POR n : $\mathbf{Z} \to Z_n$: $z \to \overline{z}$.

He aquí la partición de **Z** definida por la aplicación RESTO POR **n**

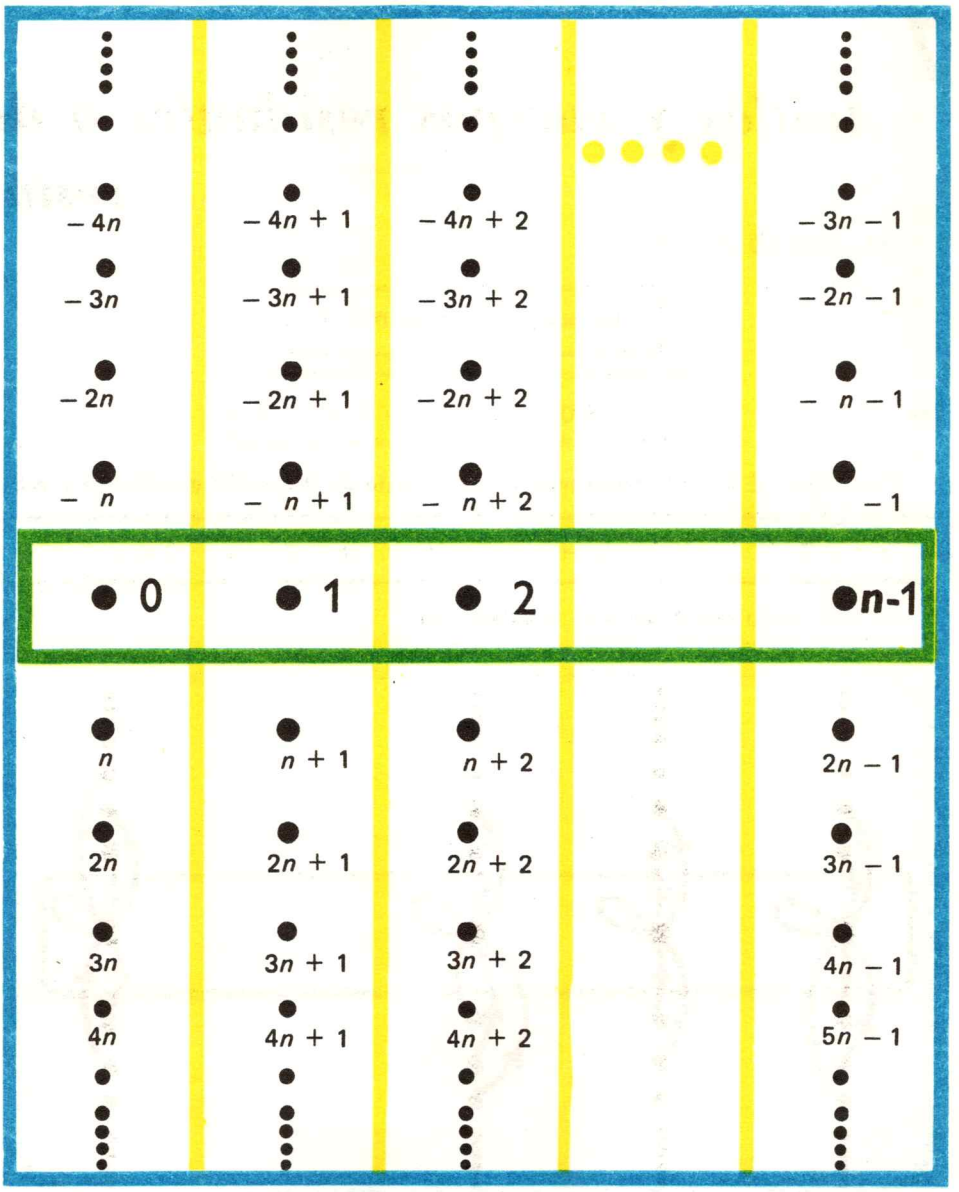
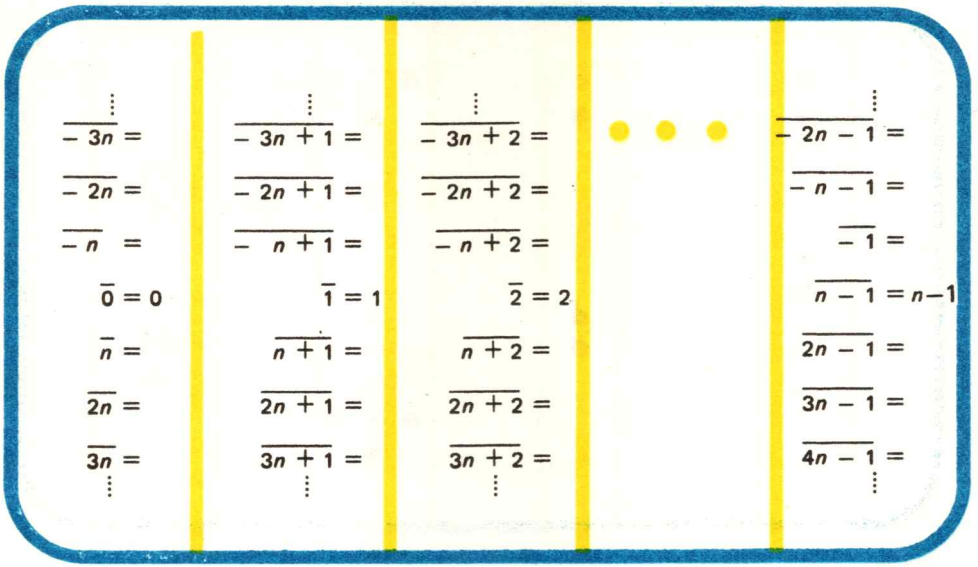


FIG. 62

Luego



$\forall\, a, b \in \mathbf{Z}$:

$$a - \bar{a} \in \text{mod } n$$

$$\bar{a} = \bar{b} \iff a - b \in \text{mod } n$$

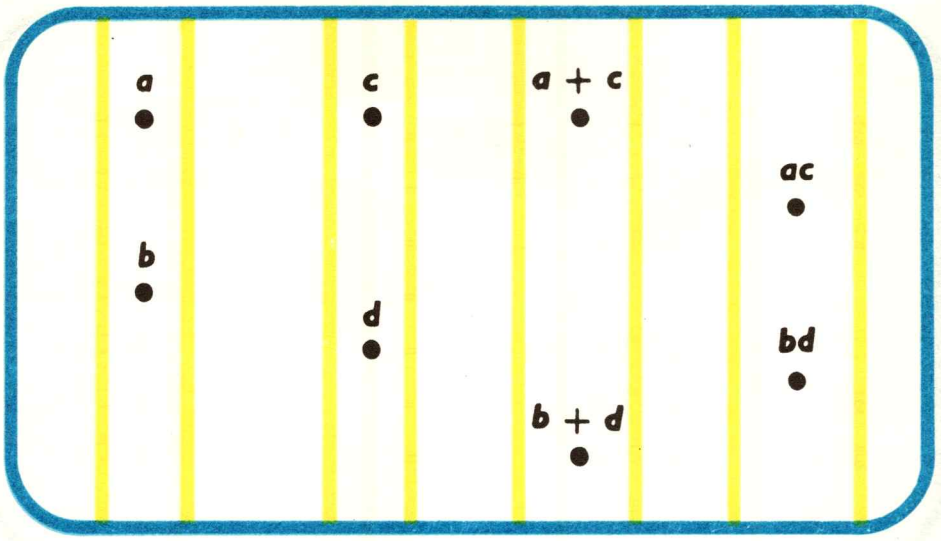
$$\mathbf{Z}_n = \{ \bar{z} \mid z \in \mathbf{Z} \}$$

PROPOSICION 1

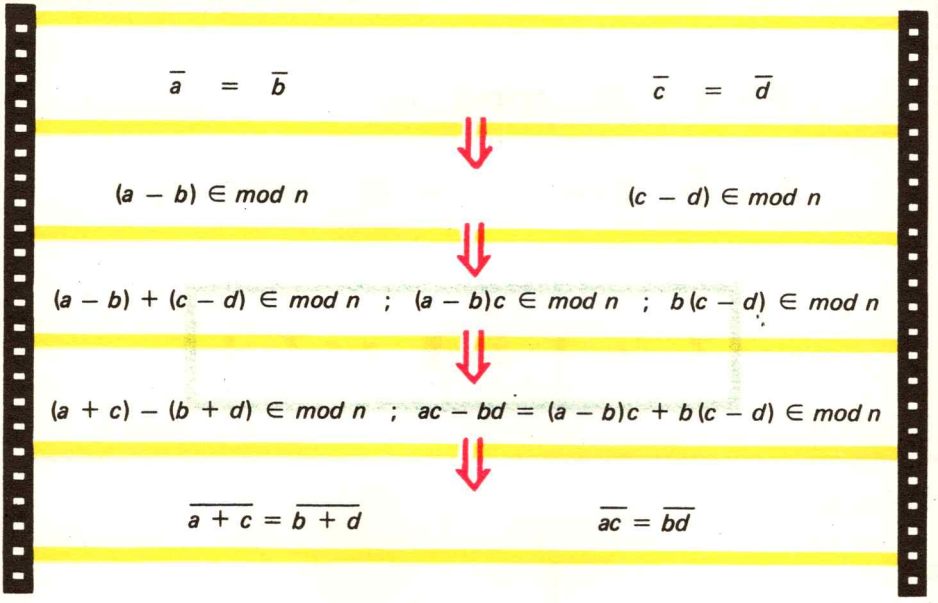
Si $a, b, c, d \in \mathbf{Z}$

Entonces $\bar{a} = \bar{b}$ y $\bar{c} = \bar{d} \Longrightarrow \overline{a + c} = \overline{b + d}$ y $\overline{a \cdot c} = \overline{b \cdot d}$

Expresado de otro modo :



DEMOSTRACION :



l. q. q. d.

Esta proposición nos permite proveer muy naturalmente al conjunto Z_n de una adición y de una multiplicación.

DEFINICION

$$\forall a, b \in \mathbf{Z}: \qquad \overline{a} + \overline{b} = \overline{a + b} \qquad \text{y} \qquad \overline{a} \cdot \overline{b} = \overline{a \cdot b}$$

El conjunto $\mathbf{Z}_n$ provisto de las leyes + y · que acabamos de definir se anota $\mathbf{Z}_n$, + , ·

Esta anotación significa

$$\forall a, b \in \mathbf{Z}_n: \qquad a + b \in \mathbf{Z}_n \qquad \text{y} \qquad a \cdot b \in \mathbf{Z}_n$$

A los efectos de evitar confusiones, los elementos de $\mathbf{Z}_n$, + , · se anotarán

$$\overline{0} \ , \ \overline{1} \ , \ \overline{2}, \ldots, \ \overline{n-1}$$

en lugar de

$$0 \ , \ 1 \ , \ 2, \ldots, \ n-1$$

— ¿Recuerdas la definición de anillos?

DEFINICION

A , + , · es un **anillo**

ssi

A , + *es un grupo conmutativo*

La multiplicación · *es asociativa*

· *distribuye* +

El anillo A , + , · *es* **conmutativo** **ssi** *su multiplicación es conmutativa.*

El anillo A , + , · *con* **unidad** **ssi** *comprende un elemento neutro no nulo para la multiplicación*

(Ese elemento neutro se llama *unidad del anillo*).

PROPOSICION 2

$$\boxed{\mathbf{Z}_n, +, \cdot \text{ es un anillo conmutativo con unidad}}$$

Los anillos $\mathbf{Z}_n$ *se llaman* **anillos de restos o anillos residuales.**

DEMOSTRACION :

1. $\mathbf{Z}_n$, + *es un grupo conmutativo*

$$\forall x, y \in \mathbf{Z}: \quad \overline{x} + \overline{y} = \overline{x + y} \in \mathbf{Z}_n$$

$$\forall x, y \in \mathbf{Z}: \quad \overline{x} + \overline{y} = \overline{x + y} = \overline{y} + \overline{x} = \overline{y} + \overline{x}$$

$$\forall x, y, z \in \mathbf{Z}: \quad \overline{x} + (\overline{y} + \overline{z})$$

$$= \overline{x} + \overline{y + z}$$

$$= \overline{x + (y + z)} = \overline{(x + y) + z}$$

$$= \overline{x + y} + \overline{z}$$

$$= (\overline{x} + \overline{y}) + \overline{z}$$

$$\forall x \in \mathbf{Z}: \quad \overline{x + 0} = \overline{x + 0} = \overline{x} = \overline{0} + \overline{x}$$

$$\forall x \in \mathbf{Z}: \quad \overline{x} + \overline{-x} = \overline{x - x} = \overline{0} = \overline{-x + x} = \overline{-x} + \overline{x}$$

$\overline{0}$ es, por lo tanto, el elemento neutro del grupo conmutativo $\mathbf{Z}_n$, +

y $\overline{-x}$ es el elemento simétrico de $\overline{x}$, lo cual nos conduce a

$$\boxed{\forall x \in \mathbf{Z}: \quad -\overline{x} = \overline{-x}}$$

2. La multiplicación es una ley interna, totalmente definida, asociativa y conmutativa.

$\forall x, y \in \mathbf{Z}$: $\quad \overline{x} \cdot \overline{y} = \overline{x\,y} \in \mathbf{Z}$

$\forall x, y \in \mathbf{Z}$: $\quad \overline{x} \cdot \overline{y} = \overline{xy} = \overline{y\,x} = \overline{y} \cdot \overline{x}$

$\forall x, y, z \in \mathbf{Z}$: $\quad \overline{x} \cdot \overline{y}\,\overline{z} = \overline{x} \cdot \overline{y\,z} = \overline{x \cdot y\,z} = \overline{x\,y \cdot z} = \overline{x\,y} \cdot \overline{z} = \overline{x}\,\overline{y} \cdot \overline{z}$

3. *La multiplicación distribuye la adición.*

$\forall x, y, z \in \mathbf{Z}$: $\quad \overline{x} \cdot (\overline{y} + \overline{z}) = \overline{x} \cdot \overline{y + z}$

$= \overline{x\,(y + z)}$

$= \overline{x\,y + x\,z}$

$= \overline{x\,y} + \overline{x\,z} = \overline{x} \cdot \overline{y} + \overline{x} \cdot \overline{z}$

4. *El elemento* $\overline{1}$ *es neutro para la multiplicación de* $\mathbf{Z}_n$, + , ·

$\forall x \in \mathbf{Z}$: $\quad \overline{1} \cdot \overline{x} = \overline{1 \cdot x} = \overline{x}$

l. q. q. d.

Luego demostraremos (c. 8 § 1) que en todo anillo, el cero, es decir el neutro para la adición es absorbente para la multiplicación. Esta propiedad se verifica directamente para los anillos $\mathbf{Z}_n$, + , ·

En efecto, para todo $x \in \mathbf{Z}$: $\quad \overline{0} \cdot \overline{x} = \overline{0 \cdot x} = \overline{0}$

Ejercicio

Justifica cada etapa de la demostración de la proposición 2.

EJERCICIOS

1. Tablas de adición y de multiplicación de $\mathbf{Z}_2$, + , ·

+	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

·	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

2. Tablas de adición y de multiplicación en $\mathbf{Z}_3$, + , ·

+	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

·	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

3. Tablas de adición y de multiplicación en $\mathbf{Z}_4$, + , ·

+	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

·	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

4. Tablas de adición y de multiplicación en $\mathbf{Z}_5$, + , ·

+	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

·	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

5. Examinando las tablas dadas, muestra que $\mathbf{Z}_2$, $\mathbf{Z}_3$, $\mathbf{Z}_5$ son cuerpos y que $\mathbf{Z}_4$ no lo es.

6. $\{0\}$ es un subanillo de $\mathbf{Z}$, + , ·

El anillo $\{0\}$, + , · no tiene unidad, aunque 0 sea el neutro para la multiplicación.

7. $\mathbf{Z}$, +, · es un anillo.

$2\mathbf{Z}$ es una parte de $\mathbf{Z}$

$2\mathbf{Z}$, + , · es un anillo para las leyes de $\mathbf{Z}$, +, ·

Es lo que se expresa diciendo que $2\mathbf{Z}$ es un subanillo de $\mathbf{Z}$, +, ·

8. Para todo $n \in \mathbf{Z}$: $n\,\mathbf{Z}$ es un subanillo de $\mathbf{Z}$, +, ·

9. Para todo número natural $n > 1$:

$\mathbf{Z}_n$ es una parte de $\mathbf{Z}$ pero no es un subanillo de $\mathbf{Z}$

$\mathbf{Z}_n$, +, · es un anillo para leyes que no son las de $\mathbf{Z}$

Por lo tanto, es sólo por abuso de anotación que las leyes de $\mathbf{Z}_n$,, +, · se anotan como las de $\mathbf{Z}$, +, ·

10. $\mathbf{Z}_2 \subset \mathbf{Z}_3 \subset \mathbf{Z}_4 \subset \mathbf{Z}_5 \subset \mathbf{Z}_6 \subset \ldots \subset \mathbf{Z}$

Cada uno de los $\mathbf{Z}_n$ es un anillo.

Ninguno de ellos es subanillo del otro.

2 – DIVISORES DE CERO

PROPOSICION 3

Si *n no es primo*

Entonces *existen elementos* $\overline{a}, \overline{b} \in \mathbf{Z}_n$ tales que

$$\overline{a} \neq \overline{0} \neq \overline{b} \qquad \text{y} \qquad \overline{a} \cdot \overline{b} = \overline{0}$$

Este hecho también se expresa diciendo que :

PROPOSICION 3

Si *n no es primo*

Entonces *el anillo* $\mathbf{Z}_n$, +, · *admite* **divisores de cero** (*no nulos*).

DEMOSTRACION :

Si *n* no es primo,

Entonces $n = a \cdot b$ donde a, b son números naturales tales que

$$1 < a < n \qquad \text{y} \qquad 1 < b < n$$

Por lo tanto

$$\overline{0} = \overline{n} = \overline{a \cdot b} = \overline{a} \cdot \overline{b} \qquad \text{y} \qquad \overline{a} \neq \overline{0} \neq \overline{b}$$

l. q. q. d.

3 – CUERPOS RESIDUALES

DEFINICION

K , +, · *es un* **cuerpo**

ssi

K· , +, · *es un anillo conmutativo*

y

el conjunto K_0 *de elementos no nulos de* K *es un grupo* K_0 , ·

PROPOSICION 4

$$\mathbf{Z}_n \ , +, \cdot \text{ es un cuerpo} \iff n \text{ es primo}$$

DEMOSTRACION DE

Si $\mathbf{Z}_n \ , +, \cdot$ es un cuerpo

Entonces el conjunto de elementos no nulos de $\mathbf{Z}_n \ , +, \cdot$ es un grupo para $\cdot$

Luego, el producto de toda cupla de elementos no nulos de $\mathbf{Z}_n$ es no nulo.

Dicho de otro modo : $\mathbf{Z}_n \ , + \ , \cdot$ no admite divisores de cero (no nulos).

Por lo tanto, en virtud de la proposición 3 : n es primo.

DEMOSTRACION DE $\Longleftarrow$

$\mathbf{Z}_n \ , +, \cdot$ es un anillo conmutativo en el cual $\overline{1}$ es neutro para la multiplicación
Prop. 2

Sólo falta probar que todo elemento **no nulo** de $\mathbf{Z}_n$
admite un *inverso* o *simétrico para la multiplicación.*

Todo elemento no nulo de $\mathbf{Z}_n$ se escribe

$$\overline{x} \qquad \text{con} \qquad x \in \mathbf{Z} \quad \text{y} \quad 0 < x < n$$

$$n \text{ primo y } x < n \implies n \wedge x = 1$$

$$\implies \exists\, n', x' \in \mathbf{Z} : \quad n'n + x'x = 1$$

De donde

$$\overline{n'n + x'x} = \overline{1}$$

$$\overline{n'n} + \overline{x'x} = \overline{1}$$

$$\overline{n'} \cdot \overline{n} + \overline{x'} \cdot \overline{x} = \overline{1}$$

$$\overline{n'} \cdot \overline{0} + \overline{x'} \cdot \overline{x} = \overline{1}$$

$$\overline{x'} \cdot \overline{x} = \overline{1}$$

l. q. q. d.

El inverso $\overline{x'}$ *de* $\overline{x}$ *se anotará* $\overline{x}^{-1}$

Reunamos las proposiciones 2 y 4 en el

TEOREMA 1

Para todo número natural $n > 1$: Z_n , +, · **es un anillo con unidad**

Z_n , +, · **es un cuerpo** $\iff$ n **primo**

En el anillo Z_n , +, · *anotaremos para todo* $m \in \omega_0$ *y para todo* $\overline{x} \in Z_n$:

$$m\overline{x} = \underbrace{\overline{x} + \ldots + \overline{x}}_{m \text{ términos}} \quad ; \quad \overline{0x} = \overline{0} \quad ; \quad \overline{x}^{m} = \underbrace{\overline{x} \cdot \ldots \cdot \overline{x}}_{m \text{ factores}} \quad ; \quad \overline{x}^{0} = \overline{1}$$

4 – EJERCICIOS

1. En $\mathbf{Z}_2$:

todo elemento es igual a su opuesto

todo elemento no nulo es igual a su inverso.

2. En $\mathbf{Z}_3$:

ningún elemento no nulo es igual a su opuesto

todo elemento no nulo es igual a su inverso.

3. En $\mathbf{Z}_4$:

$\overline{2} = -\overline{2}$ es el único elemento no nulo igual a su opuesto

$\overline{2}$ es el único divisor de cero (no nulo).

4. Existe $x \in \mathbf{Z}_n$ tal que $0 \neq x = -x$ **ssi** n es par.

5. El conjunto de divisores de cero (no nulos) de $\mathbf{Z}_6$ es $\{-\overline{2}, \overline{2}, \overline{3}\}$

6. En todo cuerpo K, +, · (cuya unidad anotaremos e) : $e^{-1} = e$

7. En $\mathbf{Z}_2$, +, · : $\overline{1}^{-1} = \overline{1}$

8. En $\mathbf{Z}_3$, +, · : $\overline{1}^{-1} = \overline{1}$ $\quad \overline{2}^{-1} = \overline{2}$

9. En $\mathbf{Z}_5$, +, · : $\overline{1}^{-1} = \overline{1}$ $\quad \overline{3}^{-1} = \overline{2}$

$\overline{2}^{-1} = \overline{3}$ $\quad \overline{4}^{-1} = \overline{4}$

10. En $\mathbf{Z}_7$, +, · calcula los inversos de $\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}$

11. En $\mathbf{Z}_{13}$, +, · resuelve las ecuaciones

$$x + \overline{5} = \overline{0}$$

$$\overline{2}\,x = \overline{1}$$

$$\overline{4}\,x = \overline{3}$$

$$\overline{6}\,x + \overline{12} = \overline{9}$$

$$\overline{3}\,x - \overline{7} = \overline{8} - \overline{9}\,x$$

¡Un buen consejo!

Previamente construye las tablas

de opuestos y de inversos en $\mathbf{Z}_{13}$

12. He aquí $\mathbf{Z}_n$ (con $n > 2$) ; $m, n \in \omega$

Si $m \wedge n = 1$ **Entonces** $\overline{m}$ es inversible en $\mathbf{Z}_n$

Si $m \wedge n \neq 1$ **Entonces** $\overline{m}$ es divisor de cero (eventualmente nulo).

13. Para todo $\overline{x} \in \mathbf{Z}_n$ (donde n es un número natural, por lo menos igual a 2) se tiene una y sólo una de las eventualidades :

1° $\overline{x}$ es inversible

2° $\overline{x}$ es un divisor de cero (eventualmente nulo).

14. El grupo multiplicativo de elementos no nulos de $\mathbf{Z}_2$ es un conjunto unitario.

15. El grupo multiplicativo de elementos no nulos de $\mathbf{Z}_3$ comprende exactamente dos elementos ... y está engendrado por $\overline{2}$

16. El grupo multiplicativo de elementos no nulos de $\mathbf{Z}_5$ comprende exactamente cuatro elementos ... y está engendrado por $\overline{2}$ (o por $\overline{3}$).

17. En $\mathbf{Z}_n$:

$\forall\, a, b, \ldots, k \in \mathbf{Z}$: $\overline{a + b + \ldots + k} = \overline{a} + \overline{b} + \overline{c} + \ldots + \overline{k}$

18. En $\mathbf{Z}_n$:

$\forall\, m \in \omega_0, \forall\, a \in \mathbf{Z}$: $\overline{ma} = m\overline{a}$

19. En $\mathbf{Z}_n$:

$\forall\, a \in \mathbf{Z}$: $\overline{-a} = -\overline{a}$

20. En $\mathbf{Z}_n$:

$\forall\, m \in \omega, \forall\, a \in \mathbf{Z}$: $\overline{ma} = m\overline{a}$ y $\overline{ma} = \overline{m} \cdot \overline{a}$

21. En $\mathbf{Z}_n$:

$\forall\, a, b, \ldots k \in \mathbf{Z}$: $\overline{a \cdot b \cdot \ldots \cdot k} = \overline{a} \cdot \overline{b} \cdot \ldots \cdot \overline{k}$

22. En $\mathbf{Z}_n$:

$$\forall a \in \mathbf{Z},\ \forall n \in \omega \quad : \quad \overline{a^n} = \overline{a}^n$$

23. $2\mathbf{Z}$, + , · es un subanillo conmutativo sin unidad de $\mathbf{Z}$, +, ·

24. $2\mathbf{Z}_6$, + , · es un subanillo conmutativo sin unidad de $\mathbf{Z}_6$, +, ·

25. $2\mathbf{Z}_9 = \mathbf{Z}_9$

26. Todos los elementos de $\mathbf{Z}_2$ son cuadrados, puesto que

$$\overline{0} = \overline{0}^2 \quad \text{y} \quad \overline{1} = \overline{1}^2$$

27. Anotemos $\mathbf{Z}_p^2$ el conjunto de cuadrados de los elementos de $\mathbf{Z}_p$

$$\mathbf{Z}_p^2 = \{x^2 \mid x \in \mathbf{Z}_p\}$$

$$\mathbf{Z}_2^2 = \mathbf{Z}_2$$

Si p es un número natural primo distinto de 2

Entonces en $\mathbf{Z}_p$: $\overline{1} \neq -\overline{1}$

los elementos distintos $\overline{1}$ y $-\overline{1}$ tienen el mismo cuadrado,

la transformación $\mathbf{Z}_p \to \mathbf{Z}_p$: $x \to x^2$ del conjunto **finito** $\mathbf{Z}_p$ no es inyectiva.

Esta transformación no es, por lo tanto, suryectiva.

$\mathbf{Z}_p^2$ es una parte propia de $\mathbf{Z}_p$

$$\mathbf{Z}_2^2 = \mathbf{Z}_2$$

Para todo número natural primo $p > 2$:

$$\mathbf{Z}_p^2 \neq \mathbf{Z}_p$$

28. En el anillo $\mathbf{Z}_n$, +, ·

Si $\forall x \in \mathbf{Z}_n \quad : \quad 1 + x^2 \in \mathbf{Z}_n^2$

Entonces $\mathbf{Z}_n^2 = \mathbf{Z}_n$

29. Para todo número natural primo $p > 2$, $\exists x \in \mathbf{Z}_p \quad : \quad 1 + x^2 \notin \mathbf{Z}_p^2$

5 – EL CUERPO Z_p , + , ·

p es un número natural primo

En el cuerpo Z_p , +, · anotaremos

$$\forall\, \bar{a} \in Z_p \quad ; \quad \forall\, \bar{b} \in Z_p \setminus \{\bar{0}\} : \qquad \frac{\bar{a}}{\bar{b}} = \bar{a} \cdot \bar{b}^{-1} = \bar{b}^{-1} \cdot \bar{a}$$

PROPOSICION 5

Si $a, b, c, \in Z$ y $\bar{0} \neq \bar{b} \in Z_p$

Entonces $c = \dfrac{a}{b} \implies \bar{c} = \dfrac{\bar{a}}{\bar{b}}$

DEMOSTRACION :

He aquí $a, b, c \in Z$ tales que $\bar{0} \neq \bar{b} \in Z_p$

$$c = \frac{a}{b} \implies bc = a \implies \overline{bc} = \bar{a} \implies \bar{b} \cdot \bar{c} = \bar{a} \implies \bar{c} = \bar{a} \cdot \bar{b}^{-1} = \frac{\bar{a}}{\bar{b}}$$

l. q. q. d.

PROPOSICION 6

En el cuerpo Z_p , +, · (p es un número natural primo)

$$\forall k \in \{1, 2, \ldots, p-1\} : \quad \overline{k!} \neq \overline{0} \quad \text{y} \quad \overline{\binom{p}{k}} = \overline{0}$$

DEMOSTRACION :

He aquí $k \in \{1, \ldots, p-1\}$

1°
$$\overline{1} \neq \overline{0} \ , \ \overline{2} \neq \overline{0} \ , \ \ldots \ , \ \overline{k} \neq \overline{0}$$

$$\overline{k!} = \overline{1 \cdot 2 \cdot \ldots \cdot k} = \overline{1} \cdot \overline{2} \cdot \ldots \cdot \overline{k} \neq \overline{0}$$

2°
$$\binom{p}{k} = \frac{p \cdot (p-1) \cdot \ldots \cdot (p-k+1)}{k!}$$

$$\overline{\binom{p}{k}} = \frac{\overline{p \cdot (p-1) \cdot \ldots \cdot (p-k+1)}}{\overline{k!}} \qquad \text{(prop. 5)}$$

$$= \frac{\overline{p} \cdot \overline{(p-1) \cdot \ldots \cdot (p-k+1)}}{\overline{k!}}$$

$$= \frac{\overline{0} \cdot \ldots}{\overline{k!}}$$

$$= \overline{0}$$

l. q. q. d.

PROPOSICION 7

En el cuerpo $\mathbf{Z}_p$, $+$, $\cdot$

$$\forall\, \overline{x} \in \mathbf{Z}_p \quad : \quad \overline{x}^p = \overline{x}$$

$$\forall\, \overline{x} \in \mathbf{Z}_p \setminus \{\overline{0}\} \quad : \quad \overline{x}^{p-1} = \overline{1}$$

FERMAT

DEMOSTRACION :

● **Si** $a , b \in \mathbf{Z}$

Entonces $(\overline{a} + \overline{b})^p = \overline{a + b}^{\,p} = \overline{(a + b)^p}$

$$= \overline{a^p + \binom{p}{1} a^{p-1} b + \ldots + \binom{p}{k} a^{p-k} b^k + \ldots + \binom{p}{p-1} a b^{p-1} + b^p}$$

$$= \overline{a}^p + \binom{\overline{p}}{1} \overline{a^{p-1} b} + \ldots + \binom{\overline{p}}{k} \overline{a^{p-k} b^k} + \ldots + \binom{\overline{p}}{p-1} \overline{a b^{p-1}} + \overline{b}^p$$

(prop. 6) $= \overline{a}^p + \overline{0} \cdot \ldots + \ldots + \overline{0} \cdot \ldots + \ldots + \overline{0} \cdot \ldots + \overline{b}^p$

$$= \overline{a}^p + \overline{b}^p$$

Acabamos de probar que

● **Si** $\overline{a} , \overline{b} \in \mathbf{Z}_p$ **Entonces** $(\overline{a} + \overline{b})^p = \overline{a}^p + \overline{b}^p$

Se sigue inmediatamente que

● **Si** $\overline{a} , \overline{b} , \overline{c} \in \mathbf{Z}_p$

Entonces $(\overline{a} + \overline{b} + \overline{c})^p = (\overline{a} + \overline{b})^p + \overline{c}^p = \overline{a}^p + \overline{b}^p + \overline{c}^p$

● **Si** $\quad \overline{a}, \overline{b}, \ldots, \overline{q}, \overline{r} \in \mathbf{Z}_p$

Entonces $\quad (\overline{a} + \overline{b} + \ldots + \overline{q} + \overline{r})^p = \overline{a}^p + \overline{b}^p + \ldots + \overline{q}^p + \overline{r}^p$

●● Todo elemento de $\mathbf{Z}_p$ se escribe $\overline{x}$ con $x \in \omega_0$

Luego
$$\begin{aligned} \overline{x}^p &= \overline{(1 + \ldots + 1)}^p \\ &= (\overline{1} + \ldots + \overline{1})^p \\ &= \overline{1}^p + \ldots + \overline{1}^p \\ &= \overline{1} + \ldots + \overline{1} \\ &= \overline{1 + \ldots + 1} = \overline{x} \end{aligned}$$

Por lo tanto

Si $\quad \overline{x} \in \mathbf{Z}_p$ **Entonces** $\quad \overline{x}^p = \overline{x}$

Se probó que **Si** $\quad \overline{x} \neq \overline{0}$ **Entonces** $\quad \overline{x}^p = \overline{x} \Longrightarrow \overline{x}^{-1}\,\overline{x}^p = \overline{x}^{-1}\,x$

$$\Longrightarrow \overline{x}^{p-1} = \overline{1}$$

l. q. q. d.

EJERCICIOS

1. **Si** $\quad p$ es un número natural primo

   Entonces $\quad \forall\, z \in \mathbf{Z}: \quad p \mid z^p - z$ (Fermat)

2. **Si** $\quad$ el número natural primo p no divide $z \in \mathbf{Z}$

   Entonces $\quad p \mid z^{p-1} - 1$ (Fermat)

6 – MORFISMOS

$\mathbf{Z}$, +, · es un anillo conmutativo con unidad, **infinito.**

$\mathbf{Z}_n$, +, · es un anillo conmutativo con unidad, **finito.**

La aplicación $\mathbf{Z} \to \mathbf{Z}_n : z \to \overline{z}$ es **suryectiva,** pero no es **inyectiva.**

La proposición 1 afirma que esta aplicación respeta las leyes + y · ,
lo cual se expresa brevemente diciendo que se trata de un **morfismo.**

DEFINICION

He aquí los conjuntos A , +, · *y* B, +, ·
cada uno provisto de las leyes internas totalmente definidas + *y* ·

La aplicación $f : A \to B$ *es un* MORFISMO *de* A , +, · sobre B , +, ·

ssi

f *respeta las leyes* + *y* ·

ssi

$$\forall x, y \in A : \quad f(x + y) = f(x) + f(y) \quad \text{y} \quad f(x \cdot y) = f(x) \cdot f(y)$$

Los **morfismos suryectivos** *se llaman* **epimorfismos.**

Los **morfismos biyectivos** *se llaman* **isomorfismos.**

Esta definición nos permite volver a formular la

PROPOSICION 1

La aplicación $\mathbf{Z} \to \mathbf{Z}_n : z \to \overline{z}$ *es un epimorfismo de* $\mathbf{Z}$, +, · *sobre* $\mathbf{Z}_n$, +, ·

PROPOSICION 2 (generalizada).

Si $A, +, \cdot$ *es un anillo conmutativo con unidad*

$B, +, \cdot$ *es un conjunto provisto de las leyes internas totalmente definidas* $+$ *y* $\cdot$

f *es un epimorfismo de* $A, +, \cdot$ *sobre* $B, +, \cdot$

Entonces $B, +, \cdot$ *es un anillo conmutativo con unidad.*

El cero y la unidad de B *son las imágenes del cero y de la unidad de* A

DEMOSTRACION :

Basta retomar punto por punto la demostración de la proposición 2 y reemplazar en ella

el anillo conmutativo con unidad $\mathbf{Z}, +, \cdot$ por el anillo conmutativo con unidad $A, +, \cdot$

$\mathbf{Z}_n, +, \cdot$ por $B, +, \cdot$

el epimorfismo $\mathbf{Z} \to \mathbf{Z}_n : z \to \bar{z}$ por el epimorfismo $f : A \to B : x \to f(x)$

EJERCICIOS

1. He aquí un conjunto $E \neq \phi$

   $\mathcal{P}E, \Delta, \cap$ es un anillo conmutativo con unidad, donde Δ desempeña el papel de la adición y $\cap$ el de la multiplicación. El cero de este anillo es ϕ y su unidad es E

   Para toda parte no vacía S de E, la aplicación

   $\mathcal{P}E \to \mathcal{P}S : \quad X \to X \cap S$

   es un epimorfismo del anillo $\mathcal{P}E, \Delta, \cap$ sobre el anillo $\mathcal{P}S, \Delta, \cap$

2. La aplicación suryectiva $\mathbf{Z} \to 2\mathbf{Z} : \quad z \to 2z$

   es un **epimorfismo** del grupo $\mathbf{Z}, +$ sobre el grupo $2\mathbf{Z}, +$ pero no es un morfismo del anillo $\mathbf{Z}, +, \cdot$ sobre el anillo $2\mathbf{Z}, +, \cdot$

3. Para establecer la última parte del ejercicio anterior, basta observar que el anillo $2\mathbf{Z}, +, \cdot$ no tiene unidad.

4. La suryección

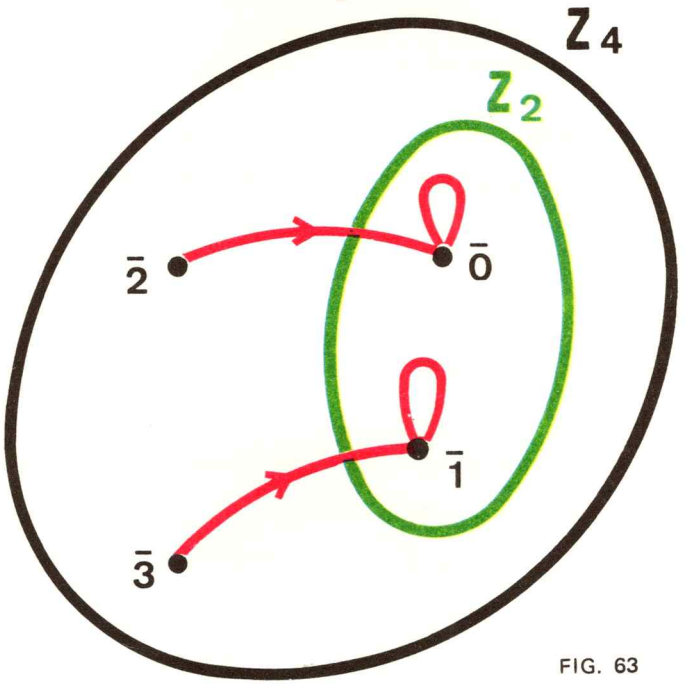


FIG. 63

es un epimorfismo de $\mathbf{Z}_4, +, \cdot$ sobre $\mathbf{Z}_2, +, \cdot$

Se observará que $\mathbf{Z}_2, +, \cdot$ no es un subanillo de $\mathbf{Z}_4, +, \cdot$

5. Define un epimorfismo $\mathbf{Z}_6 \rightarrow \mathbf{Z}_2$

6. Define otros epimorfismos de anillos residuales.

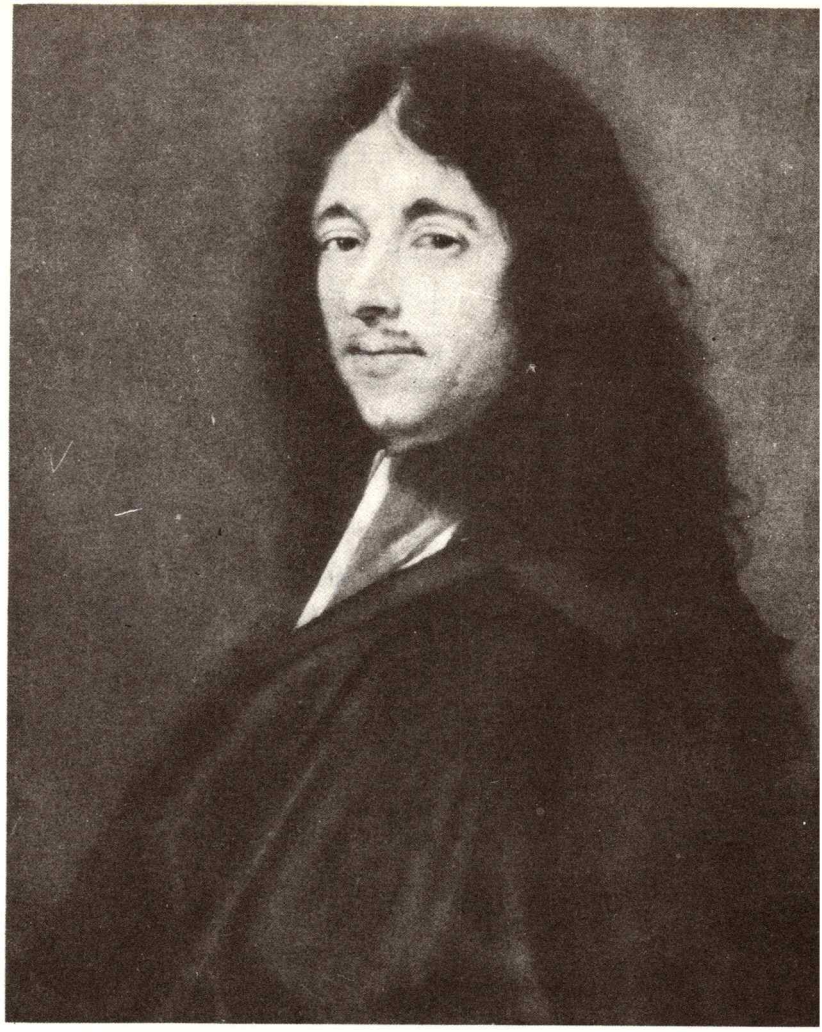
7. La transformación idéntica de todo anillo es un morfismo (y también un isomorfismo) del anillo sobre sí mismo.

8. La compuesta de toda cupla de morfismos es un morfismo.

9. La compuesta de toda cupla de epimorfismos es un epimorfismo.

10. El epimorfismo $\varphi : \mathbf{Z} \rightarrow \mathbf{Z}_n : x \rightarrow \bar{x}$

es **idempotente** : $\varphi = \varphi \circ \varphi = \varphi \circ \varphi \circ \varphi = \ldots$



PEDRO DE FERMAT (1601-1665)

Fermat nació en 1601 de una familia acomodada. Su padre, comerciante en cueros, desempeñó algunos cargos consulares. Su madre pertenecía a una familia de juristas, cuyas trazas seguirá Fermat. Estudió derecho, y una vez obtenido el título de abogado, fue nombrado magistrado en Tolouse desde la edad de 30 años. Llevó una vida de honestidad y respeto. Tuvo cinco hijos, y dos de sus hijas fueron religiosas. Sus funciones de magistrado le permitieron consagrar sus momentos de ocio a algunos placeres (lectura de autores antiguos, composición de versos en italiano y español) y también, felizmente, a la matemática y a algunas de sus aplicaciones.

Mantuvo correspondencia con Descartes, Torricelli, Roberval y Huygnens. En sus cartas propone numerosos problemas y comunica algunos de sus resultados, muchas veces de manera enigmática.

Fermat es uno de los más importantes creadores del Gran Siglo. Precursor del cálculo diferencial e integral creado por Newton y Leibniz, funda la geometría analítica con Descartes y el cálculo de probabilidades con Pascal. Su contribución más valiosa es la relativa a la teoría de números, también creada por él.

En 1640 enuncia el teorema del capítulo 7 (bajo la forma de los ejercicios 1 y 2, p. 177). Este teorema suele llamarse el PEQUEÑO TEOREMA DE FERMAT, en oposición al GRAN TEOREMA DE FERMAT, cuyo enunciado es el siguiente :

Si *el número* n *es por lo menos igual a* 3,

Entonces *no existe ninguna terna de naturales no nulos* (a, b, c) *tal que* $a^n + b^n = c^n$

No posee aún ninguna demostración completa de esta proposición (que sin embargo se pudo establecer para todo $n \leqslant 100$).

En su correspondencia, Fermat no sólo hacía alusión al "Gran Teorema" para el caso particular $n = 4$. En el margen de su DIOFANTE (un autor antiguo que se ocupaba de aritmética) Fermat escribió el enunciado de su "Gran Teorema", abregando a modo de nota que poseía una demostración admirable del mismo que no cabía en el margen de la obra.

He aquí otra proposición de Fermat, enunciada sin demostración :

Todo número natural primo de la forma $4n + 1$ *es, de manera única la suma de dos cuadrados.*

Esta proposición fue establecida por Euler en 1749.

En 1908 un profesor alemán dejó una suma de 100.000 marcos destinados a la primera persona que hiciera una demostración completa del Gran Teorema de Fermat.

Antes de tentar suerte es necesario que sepas, Amigo lector, que, como consecuencia de las sucesivas devaluaciones, esta suma no te permitiría hoy ofrecerte ni siquiera un vaso de jarabe de menta con agua.

8

Anillos conmutativos y cuerpos

1 – ANILLOS CONMUTATIVOS CON UNIDAD Y CUERPOS

Hemos encontrado numerosos ejemplos de **anillos conmutativos con unidad** y de **cuerpos.**

EJEMPLOS DE ANILLOS CONMUTATIVOS CON UNIDAD :

$\mathbb{Z}$, +, · $\quad$ $\mathbb{Z}_n$, +, · $\quad$ $\mathcal{P}E$, Δ, $\cap$ $\quad$ (con $E \neq \phi$)

El anillo L, +, · de números decimales limitados

El anillo B, +, · de números binarios limitados

Todos los cuerpos

EJEMPLOS DE CUERPOS

$\mathbb{R}$, +, · $\quad$ $\mathbb{Q}$, +, · $\quad$ $\mathbb{Z}_p$, +, · $\quad$ (*p* primo !)

En algunos de estos anillos y cuerpos, establecimos reglas de cálculo mediante un procedimiento no siempre exento de repeticiones.

Resulta económico establecer, de una vez por todas, reglas generales, válidas en todo anillo o en todo cuerpo, según el caso.

En este capítulo

A , +, · **es un anillo conmutativo con unidad**

(*anotaremos* 1 *la unidad*)

K , +, · **es un cuerpo**

2 – CERO ES ABSORBENTE

He aquí un **anillo conmutativo con unidad** $A\ ,\ +,\ \cdot$

$A, +$ es un grupo conmutativo.

Salvo convención especial, el neutro de $A\ ,\ +$ será anotado 0

(El neutro de $\mathbb{Z}_n\ ,\ +$ se anota $\overline{0}$ El neutro de $\mathcal{P}E,\ \Delta$ es ϕ)

PROPOSICION – *En todo anillo* $A\ ,\ +,\ \cdot$

el elemento 0, **neutro para la adición,** *es* **absorbente para la multiplicación.**

Dicho de otro modo :

$$\forall a \in A \qquad : \qquad a \cdot 0 = 0 = 0 \cdot a$$

(En esta fórmula, todos los 0 designan el neutro de $A\ ,\ +$)

Como consecuencia de la conmutatividad de la multiplicación, basta probar que $a \cdot 0 = 0$

DEMOSTRACION :

$$a0 = a(0+0) = a0 + a0$$

$$a0 = a0 + a0$$

$$-a0 + a0 = -a0 + a0 + a0$$

$$0 = a0$$

3 – REGLA DE LOS SIGNOS

El *opuesto,* o simétrico con respecto a la adición, de todo elemento a de A, + se anota $-a$ •

De donde $-(-a) = a$

Establezcamos la **regla de los signos**

$$\forall a, b \in A : \quad (-a)\,b = -ab = a\,(-b)$$

$$(-a)\,(-b) = ab$$

La segunda fórmula resulta inmediatamente de la primera.

Como consecuencia de la conmutatividad de la multiplicación, basta probar que

$$(-a)b = -ab$$

DEMOSTRACION :

$$(-a)b + ab = (-a + a)\,b = 0b = 0$$

$$(-a)b + ab = 0$$

Esta fórmula significa que, en el grupo A , + el elemento $(-a)\,b$ es el opuesto del elemento ab

Luego $$(-a)b = -ab$$

l. q. q. d.

4 – MULTIPLICACION ESCALAR

Es claro que

$$\begin{aligned} &\forall\, a, b \in A: && -(a+b) = -a-b \\ &\forall\, a, b, c \in A: && -(a+b+c) = -a-b-c \\ &\forall\, a, b, \ldots, q, r \in A: && -(a+b+\ldots+q+r) = -a-b-\ldots-q-r \end{aligned} \quad (1)$$

Para todo $m \in \omega_0$ y para todo $a \in A$, anotaremos

$$ma = \underbrace{a + \ldots + a}_{m \text{ términos}} \quad \text{y} \quad 0a = 0$$

Se observará que en la última fórmula, el primer 0 designa el neutro de $\mathbf{Z}$, $+$ y el segundo designa el neutro de A, $+$

La fórmula (1) implica

$$\forall m \in \omega\,; \quad \forall a \in A: \quad -(ma) = m(-a)$$

Para todo $m \in \omega_0$ y para todo $a \in A$ anotaremos

$$(-m)a = -(ma) = m(-a)$$

En particular,

$$(-1)\,a = -a$$

Acabamos de definir la **multiplicación escalar**

$$\mathbf{Z} \times A \to A : \quad (z, a) \to za$$

Un cálculo rutinario, más vale fastidioso, que el lector debe realizar hasta el final, por lo menos una vez en su vida — establece las reglas de cálculo siguientes

$\forall\, m, n \in \mathbf{Z} \quad \forall\, a, b \in A$

$(m + n)\, a$	$=$	$ma + na$	distributividad a izquierda
$mn \cdot a$	$=$	$m \cdot na$	asociatividad mixta
$m\,(a + b)$	$=$	$ma + mb$	distributividad a derecha

* * *

Solamente el grupo conmutativo $A, +$ desempeñó algún papel en este parágrafo.

Razonamientos análogos relativos al grupo conmutativo $K_0, \cdot$ introducirán las potencias con exponentes enteros racionales (elementos no nulos de un cuerpo).

Pero el conjunto de elementos no nulos de un anillo no es siempre un grupo para la multiplicación.

Definamos, pues, primero, las potencias con exponentes naturales de todo elemento del anillo conmutativo con unidad $A, +, \cdot$

5 – POTENCIAS EN UN ANILLO

Para todo $m \in \omega_0$ y para todo $a \in A$ será

$$a^m = \underbrace{a \cdot \ldots \cdot a}_{m \text{ factores}} \qquad a^0 = 1$$

a^m se llama **m-sima potencia** de a y m es el **exponente** de esta potencia.

El lector establecerá fácilmente las reglas de cálculo de las potencias

$$\forall\, m, n \in \omega\ ; \quad a \in A \ : \quad a^{m+n} = a^{m+} \cdot a^n$$

$$\forall\, m, n \in \omega\ ; \quad a \in A \ : \quad a^{mn} = (a^m)^n$$

$$\forall\, m \in \omega\ ; \quad a, b \in A \ : \quad (ab)^m = a^m\, b^m$$

6 – UNA NUEVA ASOCIATIVIDAD MIXTA

$$\forall\, m \in \mathbf{Z} \quad \forall\, a, b \in A$$

$$ma \cdot b \ \tilde{} = m \cdot ab$$

1

En esta fórmula :

el punto del primer miembro indica la multiplicación en A , + ,

el punto del segundo miembro designa la multiplicación escalar.

En el primer miembro, la multiplicación escalar ha sido anotada mediante una simple yuxtaposición, mientras que en el segundo miembro la yuxtaposición indica la multiplicación del anillo.

¡Estas son las bromas útiles de los matemáticos!

DEMOSTRACION :

1º **Si** $m = 0$

Entonces $0a \cdot b = 0 \cdot b = 0 = 0 \cdot ab$

l. q. q. d.

2º **Si** $m \in \omega_0$

Entonces $ma \cdot b = \underbrace{(a + \ldots + a)}_{m \text{ términos}} \cdot b$

$$= \underbrace{ab + \ldots + ab}_{m \text{ términos}} = m \cdot ab$$

3º **Si** $m \in -\omega_0$

Entonces $m = -n$ con $n \in \omega_0$

$ma \cdot b = (-n)a \cdot b$

$= (-na) \cdot b$ definición de la multiplicación escalar

$= -(na \cdot b)$ regla de los signos

$= -(n \cdot ab)$ nº 2

$= (-n) \cdot ab$ definición de la multiplicación escalar

$= m \cdot ab$

l. q. q. d.

Como consecuencia de la conmutatividad de la multiplicación :

$$\forall n \in \mathbf{Z} \quad \forall a, b \in A$$

$$a \cdot nb = n \cdot ab$$

2

Combinando los resultados anteriores :

$$\forall m, n \in \mathbf{Z} \quad \forall a, b \in A$$

$$ma \cdot nb = mn \cdot ab$$

ASOCIATIVIDAD MIXTA

DEMOSTRACION :

$$
\begin{aligned}
& ma \cdot nb \\
= \; & ma \cdot \boxed{nb} \\
= \; & ma \cdot \boxed{nb} && \text{Fórmula } \boxed{1} \\
= \; & m \cdot n \boxed{ab} && \text{Fórmula } \boxed{2} \\
= \; & mn \cdot \boxed{ab} && \text{Asociatividad mixta de la multiplicación escalar.} \\
= \; & mn \cdot ab
\end{aligned}
$$

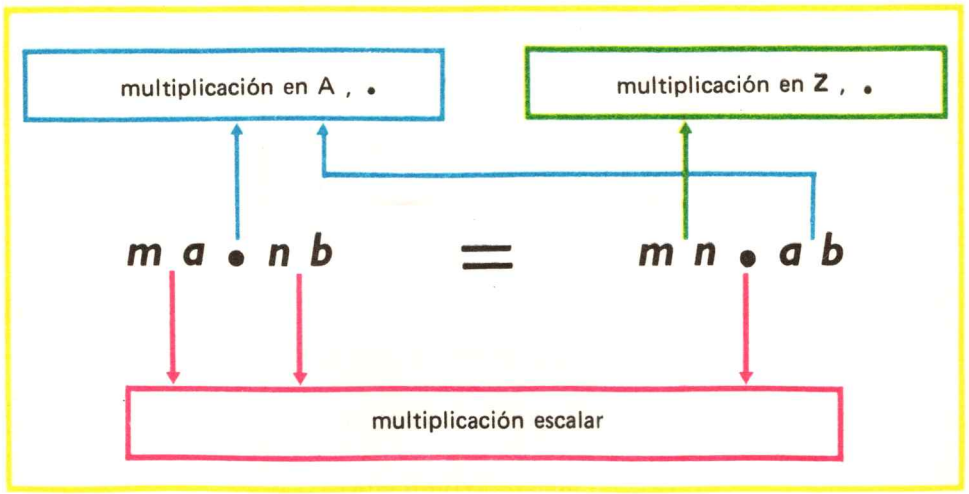
l. q. q. d.

Una vez establecidas las fórmulas anteriores, será natural indicar :

$$ma \cdot b = \mathbf{m\,a\,b} = m \cdot ab = a \cdot mb$$

y también

$$\mathbf{ma\ nb} = ma \cdot nb = mn \cdot ab = \mathbf{mn\ ab}$$



7 – DOS FORMULAS IMPORTANTES

Inspirándose en el c. 1, § 10 el lector establecerá la

Fórmula de Newton

$$\forall\, a, b \in A \quad ; \quad \forall\, m \in \omega_0 :$$

$$(a+b)^m = a^m + \binom{m}{1} a^{m-1}\, b + \ldots + \binom{m}{k} a^{m-k}\, b^k + \ldots + \binom{m}{m-1} a b^{m-1} + b^m$$

Gracias a los resultados anteriores, es fácil establecer la última regla importante de cálculo

Si $x, a \in A$ **y** $m \in \omega_0$

Entonces $x^m - a^m = (x-a)(x^{m-1} + a x^{m-2} + \ldots + a^k x^{m-k-1} + \ldots + a^{m-2} x + a^{m-1})$

DEMOSTRACION :

$$x^{m-1} + a x^{m-2} + \ldots + a^k\, x^{m-k-1} + \ldots + a^{m-2}\, x + a^{m-1}$$

$$x - a$$

$$x^m + a x^{m-1} + \ldots + a^k\, x^{m-k} + \ldots + a^{m-2}\, x^2 + a^{m-1}\, x$$

$$- a x^{m-1} - \ldots - a^k\, x^{m-k} - \ldots - a^{m-2}\, x^2 - a^{m-1}\, x - a^m$$

$$x^m \qquad\qquad - a^m$$

8 – EN LOS CUERPOS NO HAY DIVISORES DE CERO

He aquí un **cuerpo** $K, +, \cdot$

$K , +, \cdot$ es un anillo conmutativo con unidad.

Todas las convenciones y fórmulas anteriormente establecidas continúan siendo válidas.

Esta vez sabemos que el conjunto de elementos no nulos de K

$$K_0 = K \setminus \{ 0 \}$$

es un grupo para la multiplicación.

El producto de toda cupla de elementos no nulos de K es no nulo.

Esto se expresa diciendo que $K, +, \cdot$

no admite divisores de cero (no nulos).

Es decir,

$$\forall\, a, b \in K \quad : \quad (ab = 0 \quad \text{y} \quad a \neq 0) \implies b = 0$$

9 – POTENCIAS DE ELEMENTOS NO NULOS DE UN CUERPO, CON EXPONENTES ENTEROS RACIONALES

El **inverso o simétrico con respecto a la multiplicación** *de todo* $a \in K_0$

se anota a^{-1} *de donde* ... $(a^{-1})^{-1} = a$

Luego, es claro que

$$\begin{aligned} &\forall a, b \in K_0 && : (ab)^{-1} && = a^{-1} b^{-1} \\ &\forall a, b, c \in K_0 && : (abc)^{-1} && = a^{-1} b^{-1} c^{-1} \\ &\forall a, b, \ldots, q, r \in K_0 && : (ab \ldots qr)^{-1} && = a^{-1} b^{-1} \ldots q^{-1} r^{-1} \end{aligned} \qquad (2)$$

La fórmula (2) implica

$$\forall m \in \omega \quad \text{y} \quad \forall k \in K_0 : \quad (k^m)^{-1} = (k^{-1})^m$$

Para todo $m \in \omega_0$ y para todo $k \in K_0$ anotaremos

$$k^{-m} = (k^m)^{-1} = (k^{-1})^m$$

La elevación a la potencia

$$Z \times K_0 \rightarrow K_0 : (z, k) \rightarrow k^z$$

que se acaba de definir, utiliza la estructura de grupo K_0 , $\cdot$ del mismo modo que la definición de multiplicación escalar utilizaba la estructura de grupo A , +

Por lo tanto, las reglas de cálculo de las potencias con exponentes enteros racionales se obtienen, mediante una simple traducción, a partir de las reglas de cálculo de la multiplicación escalar.

$\forall m, n \in Z \qquad \forall a, b \in K_0$

$$\begin{aligned} a^{m+n} &= a^m \cdot a^n \\ a^{mn} &= (a^m)^n \\ (a\,b)^m &= a^m\, b^m \end{aligned}$$

$\forall m \in \omega_o, \forall a \in A$

$0a = 0$	$a^0 = 1$
$1a = a$	$a^1 = a$
$2a = a+a$	$a^2 = a \cdot a$
$ma = \underbrace{a+a+\ldots+a}_{m \text{ términos}}$	$a^m = \underbrace{a \cdot a \cdot \ldots \cdot a}_{m \text{ factores}}$
$-(ma) = m(-a)$	
$(-m)a = -(ma)$	

$\forall m \in \omega_o, \forall a \in K_o$

$0a = 0$	$a^0 = 1$
$1a = a$	$a^1 = a$
$2a = a+a$	$a^2 = a \cdot a$
$ma = \underbrace{a+a+\ldots+a}_{m \text{ términos}}$	$a^m = \underbrace{a \cdot a \cdot \ldots \cdot a}_{m \text{ factores}}$
$-(ma) = m(-a)$	$(a^m)^{-1} = (a^{-1})^m$
$(-m)a = -(ma)$	$a^{-m} = (a^m)^{-1} = (a^{-1})^m$

10 – EJERCICIOS

A designa un anillo conmutativo con unidad

1. Si $a \in A$

Entonces la fórmula $0\,a = 0$ se interpreta de dos maneras.
El segundo cero designa siempre el neutro de A , $+$
La fórmula es válida cuando el primer cero designa el neutro de A , $+$ o el de $\mathbf{Z}$, $+$

Realiza observaciones análogas con respecto a las fórmulas

$$1\,a = a$$

$$(-1)\,a = -a$$

2. Si $a, b, x, y \in A$; $m, n, p \in \omega$

Entonces $a\,x^m\,y^n \cdot b\,x^p\,y^q = ab\,x^{m+p}\,y^{n+q}$

3. Si $m \in \mathbf{Z}$ y $0 \in A$

Entonces $m\,0 = 0$

4. Si 1 es la unidad de A

Entonces $\forall n \in \omega : \quad 1^n = 1$

5. La multiplicación escalar en los anillos, satisface la regla de los signos.

$\forall\, m \in \mathbf{Z}$, $\forall a \in A$: $\quad (-m)\,a = m\,(-a) = -(ma)$

$$(-m)\,(-a) = ma$$

6. En el cuerpo K , $+$, $\cdot$ (cuya unidad anotamos 1)

$\forall\, m \in \mathbf{Z}$: $\quad 1^m = 1$

$\forall\, m \in \mathbf{Z}$, $\forall k \in K_0$: $\quad k^{-m} = (k^{-1})^m = (k^m)^{-1}$

$$(k^{-1})^{-m} = k^m$$

7. Si a , $b \in A$

Entonces
$$a^2 - b^2 = (a-b)(a+b)$$
$$a^3 - b^3 = (a-b)(a^2 + ab + b^2)$$
$$a^4 - b^4 = (a-b)(a^3 + a^2 b + b^3)$$

8. Si $a \in A$ y $n \in \omega$

Entonces n par $\Rightarrow$ $(-a)^n = a^n$

n impar $\Rightarrow$ $(-a)^n = -a^n$

9. Si $a, b \in A$

Entonces $a^3 + b^3 = (a + b)(a^2 - ab + b^2)$

$a^5 + b^5 = \ldots$

10. Si $a, b \in A$ y $2 \neq n \in \omega$

Entonces $a^n + b^n = (a + b)(a^{n-1} - a^{n-2} b + a^{n-3} b^2 - a^{n-4} b^3 + \ldots)$

11. Si $a, b \in A$ y $n \in \omega_0$

Entonces

$$(a - b)^n = a^n - \binom{n}{1} a^{n-1} b + \binom{n}{2} a^{n-2} b^2 - \ldots + (-1)^k \binom{n}{k} a^{n-k} b^k + \ldots + (-1)^n b^n$$

11 – EL ANILLO DE LAS APLICACIONES DE UN CONJUNTO E EN UN ANILLO A, +, ·

Expondremos un método que permite fabricar nuevos anillos a partir de un anillo dado.

He aquí un anillo conmutativo con unidad $A , + , \cdot$ y un conjunto E

Recordemos que A^E designa el conjunto de aplicaciones de E en A

En símbolos :

$$A^E = \{ f : E \to A \}$$

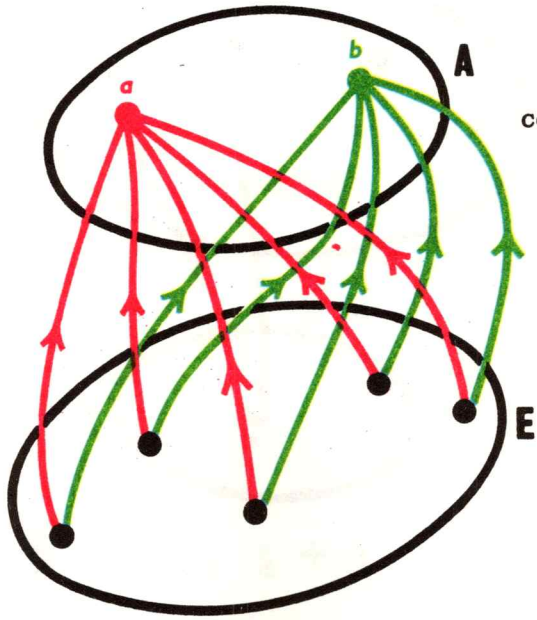
$$\forall f, g \in A^E : \quad f = g \iff \big(\forall x \in E : \quad f(x) = g(x)\big)$$

Todo elemento $a \in A$ define la función constante

$$E \to A : x \to a$$

Anotaremos esta función

$$a : E \to A : x \to a$$



LAS FUNCIONES CONSTANTES **a** Y **b**

FIG. 64

$$a : E \to A : x \to a \quad ; \quad b : E \to A : x \to b$$

De este modo se ha identificado todo elemento a de A con la función constante

$$E \to A \quad : x \to a$$

que ese elemento define.

Por lo tanto

$$A \subset A^E$$

Convertiremos A^E en un anillo conmutativo con unidad.

Para ello, debemos definir la suma y el producto de dos funciones $E \to A$ y probar que A^E provisto de estas leyes es un anillo $A^E, +, \cdot$

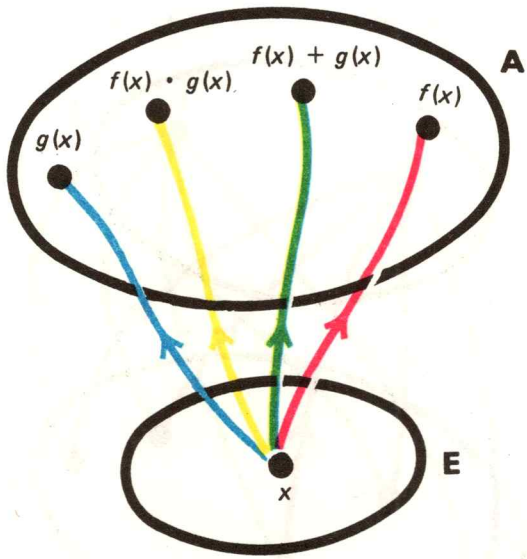
DEFINICION :

Si $f, g \in A^E$

Entonces

$$f + g : \quad E \to A : \quad x \to \quad (f + g)(x) = f(x) + g(x)$$

$$f \cdot g : \quad A \to A : \quad x \to \quad (f \cdot g)(x) = f(x) \cdot g(x)$$



f , g , $f+g$, $f \cdot g \in A^E$

ADICION Y MULTIPLICACION EN A^E

FIG. 65

TEOREMA 1

Si $A, +, \cdot$ **es un anillo conmutativo con unidad y E es un conjunto,**

Entonces $A^E, +, \cdot$ **es un anillo conmutativo con unidad que amplía** $A, +, \cdot$

DEMOSTRACION :

Acabamos de observar que

$$\forall f, g \in A^E : \qquad f + g \in A^E \qquad \text{y} \qquad f \cdot g \in A^E$$

Establezcamos que la adición y la multiplicación definidas en A^E son conmutativas y asociativas :

He aquí $f, g, h \in A^E$ y $x \in E$

1 — *Conmutatividad de la adición en* A^E

$$\begin{aligned} (f+g)(x) &= f(x) + g(x) && \text{(definición de la adición en } A^E) \\ &= g(x) + f(x) && (A, + \text{ es conmutativo}) \\ &= (g+f)(x) && \text{(definición de la adición en } A^E) \end{aligned}$$

Luego $$f + g = g + f$$

2 — *Conmutatividad de la multiplicación en* A^E

$$\begin{aligned} (fg)(x) &= f(x)\, g(x) && \text{(definición de la multiplicación en } A^E) \\ &= g(x)\, f(x) && (A, + \text{ es conmutativo}) \\ &= (gf)(x) && \text{(definición de la multiplicación en } A^E) \end{aligned}$$

Luego $$f g = g f$$

3 — *Asociatividad de la adición en* A^E

$$\big((f + g) + h\big)\ (x)$$

$$= \quad (f + g)(x) + h(x) \qquad \text{(definición de la adición en } A^E\text{)}$$

$$= \quad \big(f(x) + g(x)\big) + h(x) \qquad \text{(definición de la adición en } A^E\text{)}$$

$$= \quad f(x) + \big(g(x) + h(x)\big) \qquad \text{(asociatividad de A , +)}$$

$$= \quad f(x) + (g + h)(x) \qquad \text{(definición de la adición en } A^E\text{)}$$

$$= \quad \big(f + (g + h)\big)\ (x) \qquad \text{(definición de la adición en } A^E\text{)}$$

Luego $\boxed{(f + g) + h \;=\; f + (g + h)}$

4 — *Asociatividad de la multiplicación en* A^E

$$(fg \cdot h)(x)$$

$$= \quad (fg)(x) \cdot h(x)$$

$$= \quad f(x)g(x) \cdot h(x)$$

$$= \quad f(x) \cdot g(x)h(x)$$

$$= \quad f(x) \cdot (gh)(x)$$

$$= \quad (f \cdot gh)(x)$$

¡Justifica!

Luego $\boxed{fg \cdot h \;=\; f \cdot gh}$

5 — *La función nula* $0 : E \to A : x \to 0$

es neutro para la adición de A^E

Como consecuencia de la conmutatividad de la adición en A^E, basta probar que $f + 0 = f$

$(f + 0)(x) = f(x) + 0(x)$ (definición de la adición en A^E)

$= f(x) + 0$ (definición de la función $0 \in A^E$)

$= f(x)$ (0 es neutro de A , +)

Luego $f + 0 = f = 0 + f$

6 — *La función* 1 : $E \to A : x \to 1$

es neutro para la multiplicación de A^E

Como consecuencia de la conmutatividad de la multiplicación en A^E, basta probar que $f \cdot 1 = f$

$(f \cdot 1)(x) = f(x) \cdot 1(x)$

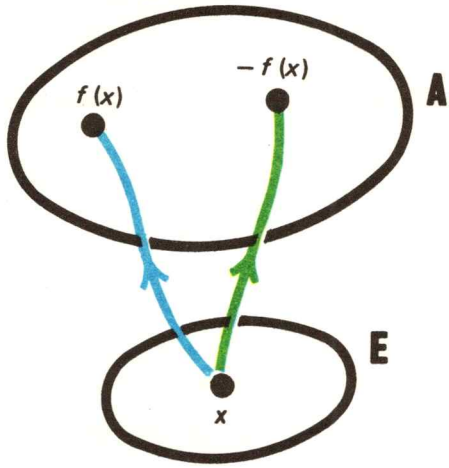
$= f(x) \cdot 1$ ¡Justifica!

$= f(x)$

Luego $f \cdot 1 = f = 1 \cdot f$

7 – *Llamemos* $-f$ *a la función* $E \to A : x \to -f(x)$

Así, $\forall x \in E : \quad (-f)(x) = -f(x)$



f ; $-f$

LA FUNCION f Y SU OPUESTA – f

FIG. 66

Mostremos que $-f$ es la opuesta de f en $A^E, +$

Como consecuencia de la conmutatividad de la adición en A^E, basta probar que $-f + f = 0$

$(-f + f)(x) = (-f)(x) + f(x)$ (definición de la adición en A^E)

$= -f(x) + f(x)$ (definición de $-f$)

$= 0$ ($-f(x)$ es el opuesto de $f(x)$ en $A, +$)

Luego $\boxed{-f + f = 0 = f - f}$

8 – *Teniendo en cuenta* 1 , 3 , 5 , 7 , *hemos probado que*

$\boxed{A^E, + \text{ es un grupo conmutativo}}$

9 — *La multiplicación de* A^E *distribuye la adición de* A^E

$$
\begin{aligned}
&\big((f + g)h\big)\,(x) \\
&= (f + g)(x) \cdot h(x) && \text{(definición de la multiplicación en } A^E) \\
&= \big(f(x) + g(x)\big) \cdot h(x) && \text{(definición de la adición en } A^E) \\
&= f(x)h(x) + g(x)h(x) && (\cdot \text{ distribuye } + \text{ en } A, +, \cdot) \\
&= (fh)(x) + (gh)(x) && \text{(definición de la multiplicación en } A^E) \\
&= (fh + gh)(x) && \text{(definición de la adición en } A^E)
\end{aligned}
$$

Luego $\qquad (f + g)\,h = f\,h + g\,h$

10 — *Teniendo en cuenta* 8 , 2,, 4 , 6 , 9 , *establecimos que*

$A^E, +, \cdot$ **es un anillo conmutativo con unidad.**

11 — *La adición y la multiplicación de* $A^E, +, \cdot$ *amplían la adición y la multiplicación de* $A, +, \cdot$

He aquí $a, b \in A$

Designemos excepcionalmente con α y β las funciones constantes definidas por a y b

$$\alpha : E \to A : x \to a \qquad ; \qquad \beta : E \to A : x \to b$$

Debemos probar que la suma $\alpha + \beta$ de las funciones α, β es la función constante definida por $a + b$

y que el producto $\alpha\,\beta$ de las funciones α, β es la función constante definida por $a\,b$

$$
\begin{aligned}
(\alpha + \beta)(x) &= \alpha(x) + \beta(x) && \text{(definición de la adición en } A^E) \\
&= a + b && \text{(definición de } \alpha, \beta) \\
(\alpha\,\beta)\,(x) &= \alpha(x) \cdot \beta(x) && \text{(definición de la multiplicación en } A^E) \\
&= ab && \text{(definición de } \alpha, \beta)
\end{aligned}
$$

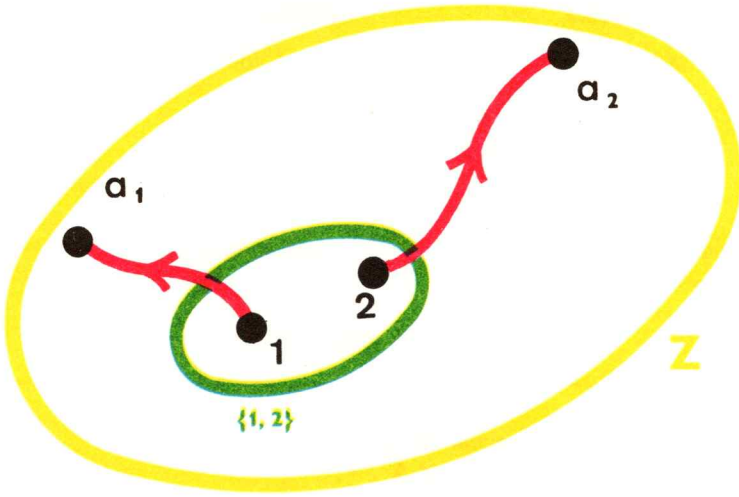
l. q. q. d.

En particular, el conjunto A^A de transformaciones de A es un anillo conmutativo con unidad.

$A^A, +, \cdot$ **es un anillo conmutativo con unidad.**

EJERCICIOS

1. El conjunto $Z^{1,2}$ se identifica claramente con el conjunto $Z^2 = Z \times Z$ de cuplas de elementos de Z



$$(a_1 , a_2) \in Z^{\{1,2\}} = Z^2 = Z \times Z$$

FIG. 67

Define la adición y la multiplicación en Z^2 , + , ·

$\forall\, a, b, c, d \in Z$: $\quad (a, b) + (c, d) = (a + c, b + d)$

$$(a, b) \cdot (c, d) = (ac , bd)$$

¿Cuál es el cero de este anillo?

Calcula $-(a, b)$

Resuelve la ecuación $\quad (x, y) + (2, -25) = (-17, 33)$

¿Cuál es la unidad de este anillo?

Sean

$$Z' = \{ (a, 0) \mid a \in Z \},$$

$$Z'' = \{ (0, b) \mid b \in Z \}$$

$$Z''' = \{ (a, a) \mid a \in Z \}$$

Las biyecciones $p' : \mathbf{Z} \to \mathbf{Z}' : x \to (x, 0)$

$p'' : \mathbf{Z} \to \mathbf{Z}'' : x \to (0, x)$

$p''' : \mathbf{Z} \to \mathbf{Z}''' : x \to (x, x)$

son isomorfismos del anillo $\mathbf{Z}, +, \cdot$ sobre los anillos conmutativos con unidad $\mathbf{Z}', +, \cdot$; $\mathbf{Z}'', +, \cdot$; $\mathbf{Z}''', +, \cdot$

La unidad de $\mathbf{Z}'$ es $(1, 0)$

de $\mathbf{Z}''$ es $(0, 1)$

de $\mathbf{Z}'''$ es $(1, 1)$

Se observará que las unidades de $\mathbf{Z}'$ y de $\mathbf{Z}''$ son distintas de la unidad de $\mathbf{Z}^2$

$\mathbf{Z}'$, $\mathbf{Z}''$, $\mathbf{Z}'''$ son **subanillos** de $\mathbf{Z}^2$, $+, \cdot$

$$\mathbf{Z}' \cap \mathbf{Z}'' = \{ \ (0, 0) \}$$

$$\mathbf{Z}' + \mathbf{Z}'' = \{ (a, 0) + (0, b) \ \blacksquare \ a, b \in \mathbf{Z} \} = \mathbf{Z}^2$$

$$\mathbf{Z}' \cdot \mathbf{Z}'' = \{ (a, 0) \cdot (0, b) \ \blacksquare \ a, b \in \mathbf{Z} \} = \{ (0, 0) \}$$

Todo elemento $(a, b) \in \mathbf{Z}^2$ se escribe de manera única como suma de un elemento de $\mathbf{Z}'$ y de un elemento de $\mathbf{Z}''$

$\mathbf{Z}$ es un anillo sin divisores de cero no nulos.

$$(a, b)\cdot(c, d) = (0, 0) \iff \big((a = 0 \text{ ó } c = 0) \text{ y } (b = 0 \text{ ó } d = 0)\big)$$

$\mathbf{Z}' \cup \mathbf{Z}''$ es el conjunto de divisores de cero (la cupla $(0, 0)$ comprendida) de $\mathbf{Z}^2$

2. Realiza un estudio análogo con respecto al anillo $\mathbf{Z}^3, +, \cdot$

3. **Si** $A, +, \cdot$ es un anillo conmutativo con unidad y E es un conjunto no vacío

Entonces $A \to A^E : a \to$ (función constante $E \to A : x \to a$) es un morfismo inyectivo del anillo $A , + , \cdot$ en el anillo $A^E, +, \cdot$

4. Para todo conjunto unitario E, el anillo $A^E, +, \cdot$ es isomorfo al anillo $A , +, \cdot$

5. He aquí una parte no vacía S del conjunto E y un anillo conmutativo con unidad $A , +, \cdot$

Para toda $f \in A^E$, designaremos con f_S la restricción de f a S, es decir, la función $f_S \in A^S$ definida por

$$\forall x \in S : \quad f_S(x) = f(x)$$

Así queda definida la suryección $A^E \to A^S : f \to f_S$ que es un epimorfismo del anillo $A^E, +, \cdot$ sobre el anillo $A^S, +, \cdot$

9

Funciones polinomios de un Anillo

1 – FUNCIONES POLINOMIOS DE UN ANILLO

He aquí un anillo conmutativo con unidad $A, +, \cdot$

DEFINICION

f es una **función polinomio** *de* A

ssi

$$f: \quad A \to A: \quad x \to f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0$$

donde $n \in \omega$ y los $a_i \in A$

La función polinomio f que acabamos de introducir se anotará de manera abreviada

$$"a_n\, x^n + a_{n-1} x^{n-1} + \ldots + a_1\, x + a_0"$$

Designaremos con [A] el conjunto de funciones polinomios de A

EJEMPLOS

1. La función $f : \mathbf{R} \to \mathbf{R} : x \to 7x^3 - 2x^2 + 2x + 5$ es una función polinomio de **R** y se anotará, abreviadamente, "$7x^3 - 2x^2 + 2x + 5$"

2. La función $f : \mathbf{Z} \to \mathbf{Z} : x \to 4x^9 - 8x^7 + 3x^4 - 2x + 1$ es una función polinomio de **Z** y de manera abreviada la anotaremos
$$"4x^9 - 8x^7 + 3x^4 - 2x + 1"$$

3. Para todo elemento a del anillo conmutativo con unidad A la transformación constante $a : A \to A : x \to a$ es una función polinomio de A que abreviadamente, se anotará "a" o más simplemente a

   Se identifica de esta manera todo elemento de A con el polinomio constante que él define
$$A \subset [A]$$

4. Toda función polinomio de A es una transformación de A
$$[A] \subset A^A$$

5. $$A \subset [A] \subset A^A$$

6. La transformación idéntica de A
$$1_A : A \to A : x \to x$$
es una función polinomio de A

   Abreviadamente la anotaremos "x"
$$1_A = "x" \in [A]$$

7. La función $1 : A \to A : x \to 1$ es una función polinomio de A que anotaremos "1" o 1
$$1 = "1" \in [A]$$

¡ATENCION! No confundir $1_A = "x"$ y $1 = "1"$

$1_A = "1"$ es la *transformación idéntica* $A \to A : x \to x$

$1 = "1"$ es la *transformación constante* $A \to A : x \to 1$

8. La función nula $\quad A \to A \ : \ x \to 0$

es la función polinomio de A anotada "0" ó 0

9. Habiendo fijado el anillo conmutativo con unidad $\quad A\ ,\ +,\ \cdot$

"x^2" designa la función polinomio $\quad A \to A : x \to x^2$

Para todo $a \in A$:

"$x - a$" designa la función polinomio $\quad A \to A : x \to x - a$

"$x^n - a^n$" designa la función polinomio $\quad A \to A : x \to x^n - a^n$

10. La sucesión $a_0, a_1, \ldots, a_n$ de elementos de A determina la función polinomio

$$f : \ A \to A : \quad x \to a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$

que también se anota

$$"a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0"$$

11. La función polinomio del cuerpo $\mathbf{Z}_p$

$$"x^p - x" : \ \mathbf{Z}_p \to \mathbf{Z}_p \ : \ x \to x^p - x$$

es la función nula.

Luego, en $[\mathbf{Z}_p]$: $\qquad "x^p - x" = 0$

12. La función polinomio del cuerpo $\mathbf{Z}_p$

$$"x^p" : \ \mathbf{Z}_p \to \mathbf{Z}_p : \ x \to x^p$$

es la transformación idéntica de $\mathbf{Z}_p$

Luego, en $[\mathbf{Z}_p]$: $\qquad "x^p" = "x"$

13. La función polinomio "x^{p-1}" del cuerpo $\mathbf{Z}_p$

$$"x^{p-1}" : \ \mathbf{Z}_p \to \mathbf{Z}_p : \ x \to x^{p-1}$$

no es la función constante $\overline{1}$

14. Para todo $x \in \mathbf{Z}_3$:

$$x^3 = x \qquad \text{(Fermat)}$$
$$x^4 = x^2$$
$$x^5 = x^3 = x$$
$$x^6 = x^2$$
$$x^7 = x^3 = x$$

... etc.

Luego $x = x^3 = x^5 = x^7 = \ldots$

$x^2 = x^4 = x^6 = x^8 = \ldots$

Toda función polinomio de $\mathbf{Z}_3$ se escribe "$ax^2 + bx + c$" con $a, b, c \in \mathbf{Z}_3$

15. $[\mathbf{Z}_2] = \{ 0, 1, \text{"}x\text{"}, \text{"}x + 1\text{"} \}$

0 y 1 son constantes; "x" y "$x + 1$" son permutaciones

$$\mathbf{Z}_2{}^{\mathbf{Z}_2} = [\mathbf{Z}_2]$$

Toda transformación de $\mathbf{Z}_2$ es una función polinomio.

16. Toda función polinomio del cuerpo $\mathbf{Z}_p$ se escribe

"$a_{p-1}\, x^{p-1} + \ldots + a_0$" donde los $a_i \in \mathbf{Z}_p$

17. En $\mathbf{Z}_2$:

las sucesiones $a_6 = a_5 = 1$, $a_4 = a_3 = a_2 = 0$, $a_1 = a_0 = 1$

y $b_6 = b_5 = 1$, $b_4 = 0$, $b_3 = b_2 = b_1 = b_0 = 1$

son distintas, pero definen la misma función polinomio de $\mathbf{Z}_2$

De manera precisa,

"$x^6 + x^5 + x + 1$" = "$x^6 + x^5 + x^3 + x^2 + x + 1$" = "$x + 1$"

2 – ANILLO DE FUNCIONES POLINOMIOS DE UN ANILLO

He aquí un anillo conmutativo con unidad A , +, ·

1°) **Si** $f = "a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0" \in [A]$

$g = "b_3x^3 + b_2x^2 + b_1x + b_0" \in [A]$

Entonces $\forall\, x \in A$:

$(f + g)(x)$

$= f(x) + g(x)$

$= a_4 x^4 + (a_3 + b_3) x^3 + (a_2 + b_2) x^2 + (a_1 + b_1) x + (a_0 + b_0)$

Luego $f + g = "a_4x^4 + (a_3 + b_3) x^3 + (a_2 + b_2) x^2 + (a_1 + b_1) x + (a_0 + b_0)" \in [A]$

> **Si** $f, g \in [A]$ **Entonces** $f + g \in [A]$

2°) **Si** $f = "a_n x^n + \ldots + a_1 x + a_0" \in [A]$

Entonces $-f = "-a_n x^n - \ldots - a_1 x - a_0" \in [A]$

3°) $\forall\, f, g \in [A] : f - g \in [A]$

4°) $0 \in [A]$

5°)

> [A] es un subgrupo del grupo conmutativo A^A, +

[A] , + es un grupo conmutativo.

6°) **Si** $f = ""a_3 x^3 + a_2 x^2 + a_1 x + a_0" \in [A]$

$g = "b_2 x^2 + b_1 x + b_0" \in [A]$

Entonces para todo $x \in A$:

$(f \cdot g)\ (x)$

$= f\ (x) \cdot g\ (x)$

$= (a_3 x^3 + a_2 x^2 + a_1 x + a_0) \cdot (b_2x^2 + b_1 x + b_0)$

$= a_3 b_2 x^5 + (a_3 b_1 + a_2 b_2) x^4 + (a_3 b_0 + a_2 b_1 + a_1 b_2) x^3$

$+ (a_2 b_0 + a_1 b_1 + a_0 b_2) x^2 + (a_1 b_0 + a_0 b_1) x + a_0 b_0$

Luego $f \cdot g = "a_3\, b_2\, x^5 + \ldots + (a_1\, b_0 + a_0\, b_1)\, x + a_0\, b_0" \in [A]$

Si $f, g \in [A]$ **Entonces** $f \cdot g \in [A]$

7°) $1 \in [A]$

Acabamos de establecer el

TEOREMA 1

Si $A, +, \cdot$ **es un anillo conmutativo con unidad**

Entonces el conjunto $[A]$ **de funciones polinomios de** A **es un subanillo conmutativo con unidad del anillo conmutativo con unidad** $A^A, +, \cdot$

Como consecuencia de la identificación de todo elemento de A **con la transformación constante que él define** $A, +, \cdot$ **es un subanillo de** $[A], +, \cdot$

Brevemente :

Si $A, +, \cdot$ *es un* **anillo conmutativo con unidad**

Entonces A, $[A]$, A^A *son* **anillos conmutativos con unidad**

$$A \subset [A] \subset A^A$$

EJERCICIOS

En [**R**]

1. "$2x^2 - 3x + 7$" · "$7x^6 - 3x^2 - 9$" =
   "$x - 1$" · "$x + 1$" =
   ("$x - a$")^5

2. Multiplica "x^2" y "x^3"
   "x^2" · "x^3" = "x^5" = "x^3" · "x^2"

   Compone "x^2" y "x^3"
   "x^2" ∘ "x^3" = "$(x^3)^2$"
   = "x^6"
   = "$(x^2)^3$" = "x^3" ∘ "x^2"

3. "$x + 1$" · "x^2" = "$x^3 + x^2$" = "x^2" · "$x + 1$"
   "$x + 1$" ∘ "x^2" = "$x^2 + 1$"
   "x^2" ∘ "$x + 1$" = "$(x + 1)^2$" = "$x^2 + 2x + 1$"

4. $\forall f \in [\mathbf{R}]$: "x" ∘ $f = f = f$ ∘ "x"
   $1 = 1 \circ f$; $f \circ 1 = f(1)$

5. **Si** A es un anillo conmutativo con unidad y $a \in A$

   Entonces "$x^n - a^n$" = "$x - a$" · "$x^{n-1} + a\,x^{n-2} + \ldots + a^{n-2}\,x + a^{n-1}$"

3 – DIVISIBILIDAD POR "x – a"

$A , + , \cdot$ es un anillo conmutativo con unidad

DEFINICION

$$\forall f, g \in [A]$$

$$f \mid g \iff \exists q \in [A] : \quad g = f \cdot q$$

La fórmula $f \mid g$ se lee "f divide g"

EJEMPLOS

1. Para todo $f, g \in [A]$: $f \mid fg$; $g \mid fg$; $1 \mid f$
$(-1) \mid g$; $f \mid f$; $f \mid -f$; $f \mid f + fg$

2. $\forall a \in A$: "$x - a$" | "$x^n - a^n$"

3. $\forall f \in [A]$: $0 \mid f \implies f = 0$

4. En [R] : $(0 \neq r \in \mathbf{R} \ \text{y} \ f \in [A]) \implies r \mid f$

5. **Si** $f , g_1 , h_1 , \ldots , g_n , h_n \in [A]$

Entonces $f \mid h_1 , f \mid h_2 , \ldots, f \mid h_n \implies f \mid g_1 h_1 + g_2 h_2 + \ldots + g_n h_n$

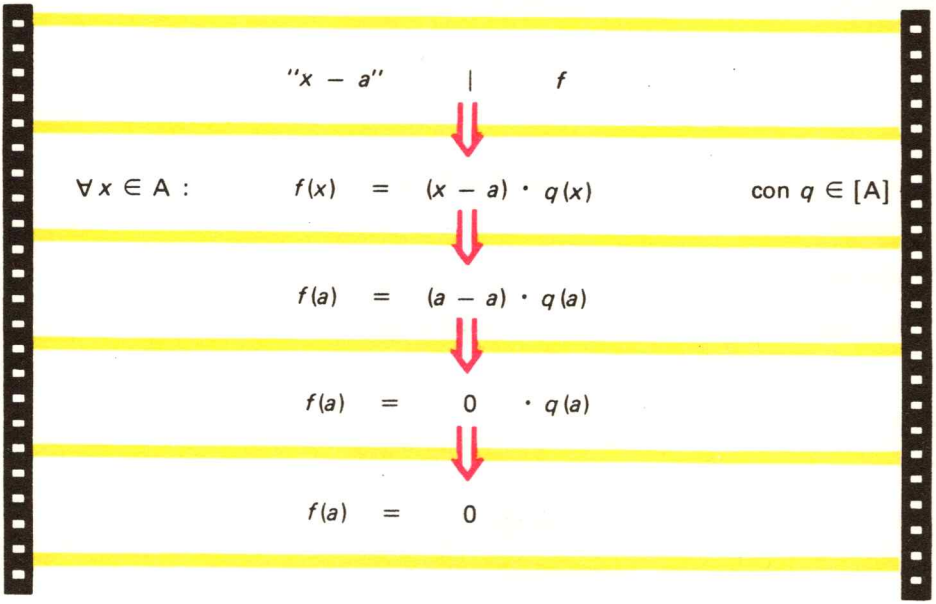
TEOREMA 2

Si **a es un elemento del anillo conmutativo con unidad A , + , ·**
y f es una función polinomio de este anillo

Entonces

$$\text{"}x - a\text{"} \mid f \iff f(a) = 0$$

DEMOSTRACION DE $\Longrightarrow$



DEMOSTRACION DE $\Longleftarrow$

He aquí $a \in A$ y $f \in [A]$ tal que $f(a) = 0$

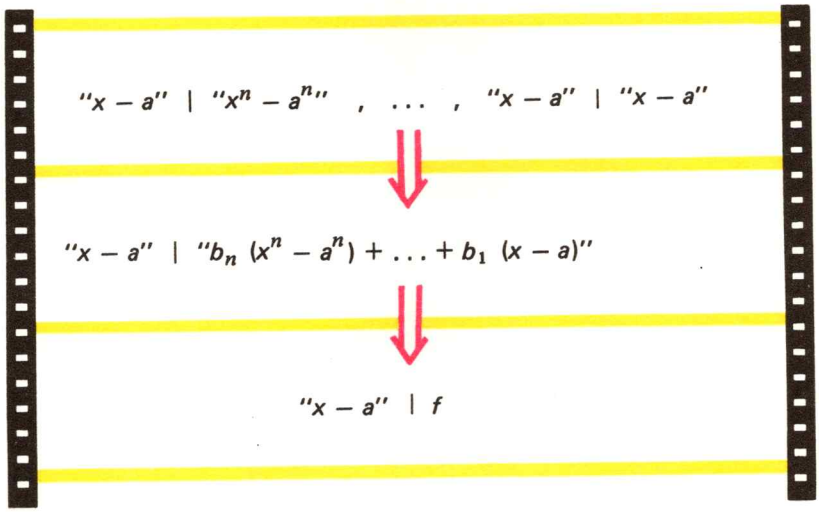
Sea $f : A \to A : x \to b_n x^n + \ldots + b_1 x_1 + b_0$

Luego

$$\forall x \in A : \quad f(x) = b_n x^n + \ldots + b_1 x + b_0$$

$$f(a) = b_n a^n + \ldots + b_1 a + b_0$$

$$\forall x \in A : \quad f(x) = f(x) - f(a) = b_n (x^n - a^n) + \ldots + b_1 (x - a)$$



l. q. q. d.

La siguiente proposición mejora el teorema 2 y da un dato sobre el cociente q

PROPOSICION 1

En [A] :

Si "$x - a$" | $f =$ "$b_n x^n + b_{n-1} x^{n-1} + \ldots + b_0$"

Entonces $f =$ "$x - a$" $\cdot$ "$b_n x^{n-1} + c_{n-2} x^{n-2} + \ldots + c_0$"

DEMOSTRACION :

En virtud del teorema 2 , la fórmula $"x - a" \mid f$ implica $f(a) = 0$

Volvamos a considerar, de manera más detallada, la segunda parte de la demostración del teorema 2

Para todo $a \in A$:

$$f(x)$$

$$= f(x) - f(a)$$

$$= b_n\,(x^n - a^n) + b_{n-1}\,(x^{n-1} - a^{n-1}) + \ldots + b_1\,(x - a)$$

$$= (x - a)\,b_n\,(x^{n-1} + a\,x^{n-2} + \ldots + a^{n-2}\,x + a^{n-1})$$

$$+ (x - a)\,b_{n-1}\,(\quad x^{n-2} + \ldots \quad)$$

$$+ (x - a)\,b_{n-2}\,(\quad x^{n-3} + \ldots \quad)$$

$$+ (x - a)\,b_2\quad(\quad x + a\,)$$

$$+ (x - a)\,b_1$$

$$= (x - a)\,(b_n\,x^{n-1} + (a\,b_n + b_{n-1})\,x^{n-2} + \ldots \quad)$$

Luego $f = "x - a" \cdot "\,b_n\,x^{n-1} + c_{n-2}\,x^{n-2} + \ldots + c_0"$

l. q. q. d.

Formulemos nuevamente el teorema 2, teniendo en cuenta la proposición 1

TEOREMA 2

En [A]

$"x - a" \mid f = "\,b_n\,x^n + b_{n-1}\,x^{n-1} + \ldots + b_0"$

ssi

$f(a) = 0$

ssi

$f = "x - a" \cdot "\,b_n\,x^{n-1} + c_{n-2}\,x^{n-2} + \ldots + c_0"$

EJERCICIOS

1. Si $f = "f_n\, x^n + \ldots + f_1\, x + f_0"$ **Entonces** $f(0) = f_0$

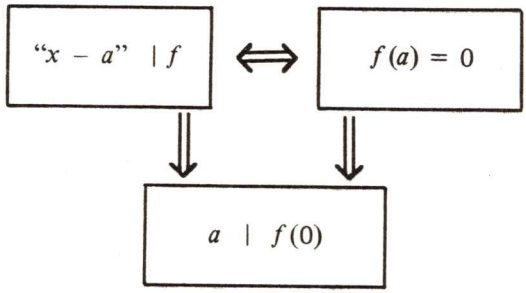
2. Si $f = "f_n\, x^n + \ldots + f_1\, x + f_0" \in [A]$ y $a \in A$

Entonces $f(a) = 0 \implies f_n\, a^n + \ldots + f_1\, a + f_0 = 0$

$\implies f_0 = -a\,(f_n\, a^{n-1} + \ldots + f_1)$

$\implies a \mid f_0$

3. En [A] :



4. Al buscar los divisores "$x - a$" de $f \in [A]$, basta considerar los "$x - a$" tales que $a \mid f(0)$

5. En [**Z**] :

Cuáles son los divisores "$x - a$" ($a \in \mathbf{Z}$) de

"$x^2 + x + 2$" "$x^2 + x + 1$" "$x^2 - x - 6$"

"$x^2 + x - 2$" "$x^2 + x - 1$" "$x^3 - 2x^2 - 13x - 10$"

4 – RAICES DE FUNCIONES POLINOMIOS

DEFINICION

He aquí una función polinomio f del anillo conmutativo con unidad A y $a \in A$

a es una **raíz** *de f*	$\Longleftrightarrow$	$f(a) = 0$

$f^{-1}\{0\}$ es, por consiguiente, el **conjunto de raíces** de *f*

EJEMPLOS Y PROPIEDADES INMEDIATAS

1. El conjunto de raíces de la función polinomio "$x^2 - 5x + 6$" de **R** es $\{2, 3\}$

2. El conjunto de raíces de la función polinomio "$x^2 - 1$" de **R** es $\{1, -1\}$

3. El conjunto de raíces de la función polinomio "x" de A es $\{0\}$

4. El conjunto de raíces de la función polinomio "$x^2 + 1$" de **R** es vacío.

5. **Si** *a* es un elemento no nulo del anillo conmutativo con unidad A , +

   Entonces el conjunto de raíces de la función polinomio *a* es vacío.

   A es el conjunto de raíces de la función polinomio nula.

6. **Si** A es un anillo conmutativo con unidad; $a \in A$; $f \in [A]$

   Entonces *a* es una raíz de *f* $\Longleftrightarrow$ "$x - a$" $\mid$ *f*

TEOREMA 3

La función polinomio del cuerpo K

$$f = \text{“}k_n x^n + \ldots + k_1 x + k_0\text{”} \quad \text{con} \quad k_n \neq 0$$

admite a lo sumo n raíces.

Además :

Si $a_1, \ldots, a_m$ **son raíces de f**

Entonces $\forall\ x \in K : \quad f(x) = (x - a_1) \cdot \ldots \cdot (x - a_m)\ q\ (x)$

con $q = \text{“}k_n x^{n-m} + q_{n-m-1} x^{n-m-1} + \ldots + q_0\text{”}$

En particular :

Si $a_1, \ldots, a_n$ **son raíces distintas de f**

Entonces $f = \text{“}k_n (x - a_1) \ldots (x - a_n)\text{”}$

DEMOSTRACION :

1. **Si** $a_1, \ldots, a_m$ son raíces distintas de f y $m \leqslant n$

Entonces $f(a_1) = 0$

$f = \text{“}(x - a_1)\, g(x)\text{”}$ con $g = \text{“}k_n x^{n-1} + \ldots\text{”}$ (prop. 7)

$f(a_2) = 0$

$(a_2 - a_1)\, g(a_2) = 0$ y $a_2 - a_1 \neq 0$

$g(a_2) = 0$ (K no admite divisor de cero)

$g = \text{“}(x - a_2)\, h(x)\text{”}$ con $h = \text{“}k_n x^{n-2} + \ldots\text{”}$ (prop. 7)

$f = \text{“}(x - a_1)(x - a_2)\, h(x)\text{”}$

$f(a_3) = 0$

$(a_3 - a_1)(a_3 - a_2)\, h(a_3) = 0$ y $a_3 - a_1 \neq 0 \neq a_3 - a_2$

$h(a_3) = 0$ (K no admite divisor de cero)

etc.

2. Si $a_1, \ldots, a_n$ son raíces distintas de f

y a es un elemento de K distinto de esas raíces

Entonces $\forall\, x \in K$: $f(x) = k_n\,(x - a_1) \ldots (x - a_n)$

$f(a) = k_n\,(a - a_1) \ldots (a - a_n)$

Pero $k_n\,,\ a - a_1\,,\ \ldots\,,\ a - a_n \in K_0$

Luego $f(a) \neq 0$

l. q. q. d.

He aquí el teorema 3 con ligeras modificaciones.

TEOREMA 3

La función polinomio del cuerpo K

$f = "k_n\, x^n + \ldots + k_1\, x + k_0"$ (los k_i no son todos nulos)

admite a lo sumo n raíces.

DEMOSTRACION :

Sea m el mayor natural tal que $k_m \neq 0$

Por consiguiente, $f = "k_m\, x^m + \ldots + k_1\, x + k_0"$ (con $k_m \neq 0$)

En virtud del teorema que acabamos de demostrar, f admite a lo sumo m, y por lo tanto a lo sumo n raíces.

l. q. q. d.

Utilizaremos el teorema 3 bajo la forma de su contrapropuesta:

TEOREMA 3

Si **la función polinomio del cuerpo K**

$f = "k_n\, x^n + \ldots + k_1\, x + k_0"$

(admite por lo menos (n + 1) raíces,

Entonces $k_n = k_{n-1} = \ldots = k_1 = k_0 = 0$

EJERCICIOS

$Z_p \setminus \{\overline{0}, \overline{1}\}$ es el conjunto de raíces de la función polinomio

$$"x^{p-2} + x^{p-3} + \ldots + x^2 + x + 1"$$

5 – EXPRESION UNICA DE CIERTAS FUNCIONES POLINOMIOS

Toda sucesión $a_n\ ,\ a_{n-1}\ ,\ \ldots\ ,\ a_1\ ,\ a_0$
de elementos de un anillo conmutativo con unidad A define la función polinomio

$$"a_n\ x^n + \ldots + a_1\ x + a_0" \in \quad [A]$$

Hemos encontrado situaciones en las cuales dos de estas sucesiones definen la misma función polinomio. Daremos con precisión ciertos casos para los cuales no se presenta dicha eventualidad.

TEOREMA 4

Si $f = "a_n x^n + \ldots + a_0"$ y $g = "b_n x^n + \ldots + b_0"$

son funciones polinomios del cuerpo K, que comprende por lo menos (n + 1) elementos

Entonces $f = g \iff a_n = b_n\ ,\ \ldots\ ,\ a_0 = b_0$

Luego, resulta que

Toda función polinomio de un cuerpo infinito K se escribe de una y sólo una manera

$$f = "a_n\ x^n + \ldots + a_0"$$

La implicación $\Longleftarrow$ es trivial.

DEMOSTRACION DE $\Longrightarrow$

$\forall\ x \in K$: $\qquad f(x) = g(x)$

$\forall\ x \in K$: $\qquad (f - g)(x) = 0$

Todo elemento de K es raíz de la función polinomio

$$f - g = "(a_n - b_n)\ x^n + \ldots + (a_1 - b_1)\ x + a_0 - b_0" \in [K]$$

Esta función admite, pues, por lo menos $n + 1$ raíces distintas.

Y, en virtud del teorema 3,

$$a_n = b_n\ ,\ \ldots\ ,\ a_1 = b_1\ ,\ a_0 = b_0$$

l. q. q. d.

PROPOSICION 2

Toda transformación f del cuerpo $\mathbf{Z}_p$, + , · (p primo)
es una función polinomio de $\mathbf{Z}_p$ *y se escribe de manera única*

$$f = "a_{p-1}x^{p-1} + \ldots + a_0"$$

DEMOSTRACION :

1. En virtud de la fórmula de Fermat (c. 7, prop. 7)

$\forall\, x \in \mathbf{Z}_p$: $x^p = x$, $x^{p+1} = x^2$, . . . , $x^{2p-2} = x^{p-1}$

$x^{2p-1} = x$, etc.

Toda función polinomio de $\mathbf{Z}_p$ se escribe, pues

$$"a_{p-1}\, x^{p-1} + \ldots + a_0"$$

y esto, de una y sólo una manera, en virtud del teorema 4

El número de funciones polinomios de $\mathbf{Z}_p$ es igual al número de sucesiones $(a_{p-1}, \ldots, a_0)$ de p elementos de $\mathbf{Z}_p$, es decir p^p

$$\#\,[\mathbf{Z}_p] = p^p$$

2. Por otra parte, sabemos (c. 1, § 3) que

$$\#\,\mathbf{Z}_p{}^{Zp} = p^p$$

3. $[\mathbf{Z}_p]$ es, por lo tanto, una parte del conjunto finito $\mathbf{Z}_p{}^{Zp}$
y comprende el mismo número de elementos que $\mathbf{Z}_p{}^{Zp}$

Luego

$$[\mathbf{Z}_p] = \mathbf{Z}_p{}^{Zp}$$

l. q. q. d.

6 – TEOREMA DE WILSON

En el anillo $\mathbf{Z}_n$, + , ·

$$\overline{(n-1)!} = -\overline{1} \iff \textbf{n primo}$$

DEMOSTRACION DE $\Longleftarrow$

Como n es primo, el anillo $\mathbf{Z}_n$, + , · es un cuerpo.

En virtud de la fórmula de Fermat (c. 7, prop. 7)

$$\forall\, x \in \mathbf{Z}_n \setminus \{\overline{0}\} \quad : \qquad x^{n-1} - \overline{1} = \overline{0}$$

Luego los $(n-1)$ elementos no nulos de $\mathbf{Z}_n$

$$\overline{1} \ , \ \overline{2} \ , \ \ldots \ , \ \overline{n-1}$$

son raíces distintas de la función polinomio "$x^{n-1} - \overline{1}$" de $\mathbf{Z}_n$

Y, en virtud del teorema 3

$$\forall\, x \in \mathbf{Z}_n \quad : \qquad x^{n-1} - \overline{1} = (x - \overline{1})\,(x - \overline{2}) \ldots (x - \overline{n-1})$$

Pero

$$\{-\overline{1}\ , \ldots , -\overline{n-1}\} = \{\overline{1}\ , \ldots , \overline{n-1}\}$$

Luego $\quad (x + \overline{1}) \cdot \ldots \cdot (x + \overline{n-1}) = (x - \overline{1}) \cdot \ldots \cdot (x - \overline{n-1})$

$$\forall\, x \in \mathbf{Z}_n \quad : \qquad x^{n-1} - \overline{1} = (x + \overline{1})\,(x + \overline{2}) \cdot \ldots \cdot (x + \overline{n-1})$$

En particular

$$\overline{0}^{n-1} - \overline{1} = (\overline{0} + \overline{1}) \cdot (\overline{0} + \overline{2}) \cdot \ldots \cdot (\overline{0} + \overline{n-1})$$

$$-\overline{1} = \overline{1} \cdot \overline{2} \cdot \ldots \cdot \overline{n-1}$$

$$\overline{(n-1)!} = -\overline{1}$$

l. q. q. d.

DEMOSTRACION DE $\Longrightarrow$

Resulta equivalente probar la implicación

n no es primo $\Longrightarrow$ $\overline{(n-1)!} \neq -\overline{1}$

-1 no es un divisor de cero de $\mathbf{Z}_n$, $+$, $\cdot$

Por lo tanto basta establecer la implicación, aparentemente más débil

n no es primo $\Longrightarrow$ $\overline{(n-1)!}$ divide cero.

Prueba :

n no es primo.

$\mathbf{Z}_n$ comprende divisores de cero no nulos (c. 7, prop. 3, p. 168)

Existen elementos no nulos $\overline{a}, \overline{b}$ de $\mathbf{Z}_n$ tales que

$$\overline{a} \cdot \overline{b} = \overline{0}$$

Pero $\overline{a}$ es uno de los factores de $\overline{2} \cdot \ldots \cdot \overline{(n-1)} = \overline{(n-1)!}$

Luego $\overline{(n-1)!} \cdot \overline{b} = \overline{0}$ con $\overline{b} \neq \overline{0}$

y $\overline{(n-1)!}$ divide cero.

l. q. q. d.

§ 7 – GRADO DE UNA FUNCION POLINOMIO DE UN CUERPO INFINITO

En § 5, vimos que para toda función polinomio no nula f del cuerpo infinito K, existe uno y sólo un entero natural n tal que f se escribe de manera única

$$f : K \to K \quad : \quad x \to k_n x^n + \ldots + k_1 x + k_0$$

donde los $k_i \in K$ y $k_n \neq 0$

El número n así definido se llama **grado de f** y se anota $d^\circ f$

Se completa la definición del grado de una función polinomio conviniendo que el grado de la función polinomio nula es $-\infty$

Por definición, el número $-\infty$ no pertenece a R, y por lo tanto tampoco a ω

Sea $\underline{\omega} = \omega \cup -\infty$

Se prolonga la estructura $\omega, +, \leqslant$ a $\underline{\omega}, +, \leqslant$ mediante las fórmulas

$$\forall x \in \omega \quad : \quad -\infty \leqslant x$$

$$\forall x \in \omega \quad : \quad -\infty + x = x + (-\infty) = -\infty$$

Estas definiciones implican inmediatamente las fórmulas

Si K es un cuerpo infinito,

Entonces para todo $f, g \in [K]$:

$$d^\circ (f + g) \leqslant \text{máx } (d^\circ f, d^\circ g)$$

$$d^\circ (fg) = d^\circ f + d^\circ g$$

En esta fórmula anterior máx $(d^\circ f, d^\circ g)$ designa el mayor de los números $d^\circ f$, $d^\circ g$. Esta fórmula se completa diciendo que

$$d^\circ f \neq d^\circ g \implies d^\circ (f + g) = \text{máx } (d^\circ f, d^\circ g)$$

Es fácil probar el

TEOREMA DE EUCLIDES

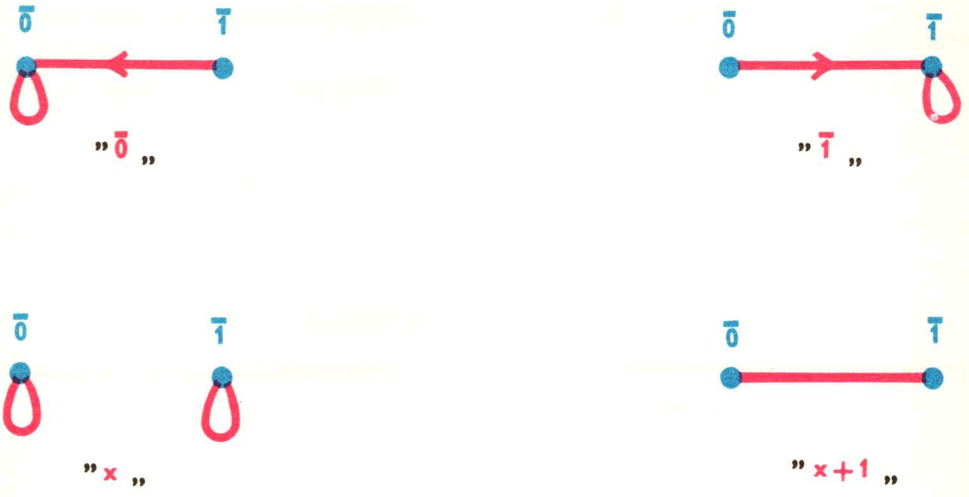
Si f, g **son funciones polinomios del cuerpo infinito K**

Entonces existe una y sólo una cupla de funciones polinomios $q, r \in [K]$ **tales que**

$$f = qg + r \quad \text{y} \quad d^\circ r < d^\circ g$$

§ 8 – EJERCICIOS

1. He aquí las cuatro funciones polinomios de Z_2



$$[Z_2] = \{"\bar{0}", \ "\bar{1}", \ "x", \ "x+\bar{1}"\} = Z_2^{Z_2}$$

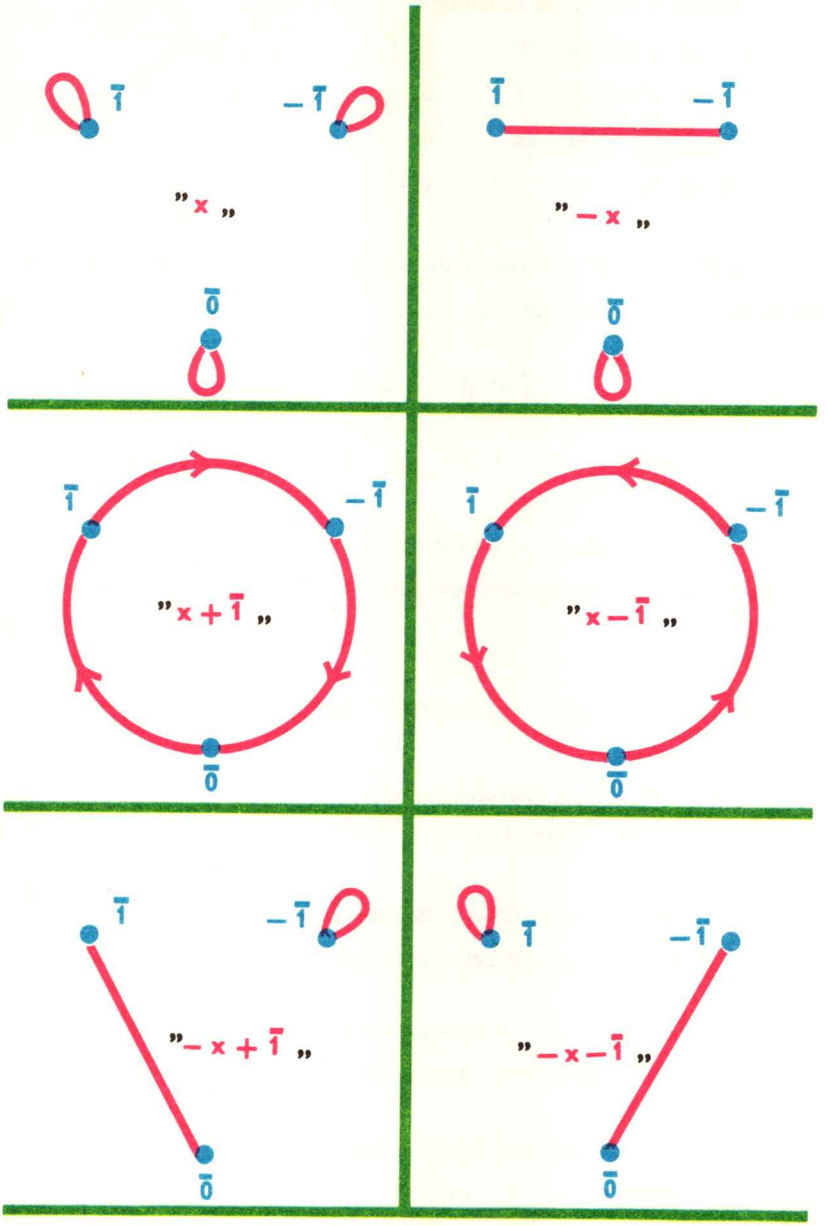
FIG. 68

2. Indica cuáles de las funciones polinomios de Z_2 son permutaciones.

3. ¿Cuántas funciones polinomios hay en Z_3?

   ¿Cuántas de ellas son permutaciones de Z_3?

4. He aquí las permutaciones de Z_3



LAS PERMUTACIONES DE Z_3

FIG. 69

5. ¿Cuáles son las raíces de las funciones polinomios de $\mathbf{Z}_2$?

El conjunto de raíces de "0" es $\mathbf{Z}_2$

El conjunto de raíces de "1" es ϕ

El conjunto de raíces de "x" es $\{0\}$

El conjunto de raíces de "$x + 1$" es $\{-1\}$

6. Toda función polinomio no constante de $\mathbf{Z}_2$ admite por lo menos una raíz.

Esto se expresa diciendo que $\mathbf{Z}_2$, + , · es un cuerpo *algebraicamente cerrado.*

7. En $\mathbf{Z}_3$, +, · $\{x^2 \mid x \in \mathbf{Z}_3\} = \{0, 1\}$

8. La función polinomio "$x^2 + 1$" de $\mathbf{Z}_3$ no admite ninguna raíz.

9. Existe una función polinomio no constante de $\mathbf{Z}_3$ que no admite ninguna raíz.

El cuerpo $\mathbf{Z}_3$ *no es algebraicamente cerrado.*

10. En $\mathbf{Z}_3$, +, ·

$\forall\, a, b \in \mathbf{Z}_3$: $a^2 + b^2 = 0 \iff a = b = 0$

11. **Si** p es un número natural primo,

Entonces $p \mid (p-1)! + 1$ (Wilson)

12. **Si** $a \in$ A y d es un divisor de cero de A

Entonces ad es un divisor de cero (eventualmente nulo).

13. **Si** $a_1, \ldots, a_n \in$ A y uno de los a_i es un divisor de cero

Entonces $a_1\, a_2 \ldots a_n$ es un divisor de cero (eventualmente nulo).

14. He aquí un número natural n por lo menos igual a 2

n primo $\iff$ $n \mid (n-1) + 1$

15. El producto de tres elementos no nulos de $\mathbf{Z}_4$ es $\overline{2}$

(Se observará que $\overline{0} \neq \overline{2} \neq -\overline{1}$)

16. Si el número natural n, por lo menos igual a 2
no es ni primo ni el cuadrado de un número primo

Entonces $\exists\ a, b \in \{2, 3, \ldots, n-1\} : \quad a \neq b \quad$ y $\quad n = ab$

17. Si el número natural n, por lo menos igual a 2
no es ni primo ni el cuadrado de un número primo

Entonces $\mathbf{Z}_n$ comprende elementos no nulos distintos $\overline{a}, \overline{b}$
tales que $\overline{a} \cdot \overline{b} = \overline{0}$

El producto de elementos no nulos de $\mathbf{Z}_n$ es $\overline{0}$

18. Si p es un número natural primo distinto de 2

Entonces
$$1 < 2 < p$$
$$p < 2p < p^2$$

19. Si p es un número natural primo distinto de 2

Entonces en $\mathbf{Z}_{p^2}$: $\quad \overline{0} \neq \overline{p} \neq \overline{2p} \neq \overline{0}$
$$\overline{p} \cdot \overline{2p} = \overline{0}$$

El producto de elementos no nulos de $\mathbf{Z}_{p^2}$ es $\overline{0}$

20. He aquí un número natural n por lo menos igual a 2

En $\mathbf{Z}_n$:

$$\overline{(n-1)!} = -\overline{1} \iff n \text{ primo}$$
$$\overline{(n-1)!} = \overline{2} \iff n = 4$$
$$\overline{(n-1)!} = \overline{0} \iff n \text{ no es ni primo ni 4}$$

LIBRO 5

PROPIEDADES ARITMETICAS DE LOS GRUPOS Y CUERPOS DE GALOIS

10

Subgrupos de un grupo

En este capítulo consideraremos a menudo un grupo cualquiera $G, *$
Anotaremos v *el neutro de este grupo, y* $\overline{g}$ *designará el simétrico del elemento* g

1 – SUBGRUPOS

DEFINICION

He aquí un conjunto E provisto de una ley $E \times E \to E : (x, y) \to x * y$ y $e \in E$

e *es un* **idempotente** *de* E , $*$ **ssi** $e * e = e$

EJEMPLOS

1. 0 es un idempotente de $\mathbf{R}, +$
2. 0 es un idempotente de $\mathbf{R}, \cdot$
3. 1 es un idempotente de $\mathbf{R}, \cdot$
4. 1 no es un idempotente de $\mathbf{R}, +$
5. El cero de todo anillo $A, +, \cdot$ es idempotente de $A, +$ y de $A, \cdot$
6. La unidad de un anillo con unidad $A, +, \cdot$ es un idempotente de $A, \cdot$
7. El neutro de un grupo $G, *$ es un idempotente de $G, *$
8. Todos los elementos de $\mathscr{P}$ E son idempotentes de $\mathscr{P}$ E, $\cap$ y de $\mathscr{P}$ E, $\cup$
9. Todos los elementos de ω son idempotentes de $\omega, \wedge$ y de $\omega, \vee$
10. Las proyecciones paralelas del plano Π son idempotentes de Π^{Π}, o (Ver MM1, c. 14, § 5, p. 221).
11. Las transformaciones constantes del conjunto E son idempotentes de E^{E}, o

PROPOSICION 1

El neutro de un grupo es su único idempotente.

DEMOSTRACION :

He aquí un grupo G , $*$ de neutro ν

$$\nu * \nu = \nu$$

ν es un idempotente de G , $*$

He aquí un idempotente e de G , $*$

$$e * e = e$$
$$\overline{e} * e * e = \overline{e} * e$$
$$e = \nu$$

l. q. q. d.

He aquí un subgrupo S del grupo G , $*$

Llamemos e al neutro de S , $*$

$$e * e = e$$

e es un idempotente de G , $*$

ν es el único idempotente de G , $*$ (prop. 1)

Luego $$e = \nu$$

De modo que el elemento neutro de un grupo es el elemento neutro de cada uno de sus subgrupos.

Demostraremos que sucede lo mismo con el simétrico.

He aquí $s \in S$

Como siempre, $\overline{s}$ designa el simétrico de s en G , $*$

Llamemos s' al simétrico de s en S

Luego $$s' * s = \nu = s * \overline{s}$$

De donde $$s' = s' * \nu = s' * s * \overline{s} = \nu * \overline{s} = \overline{s}$$

Hemos establecido así el

TEOREMA 1

Si S es un subgrupo del grupo G , $*$

Entonces el neutro de S $*$ es el de G , $*$
el simétrico en S , $*$ de todo elemento de S
es su simétrico en G , $*$

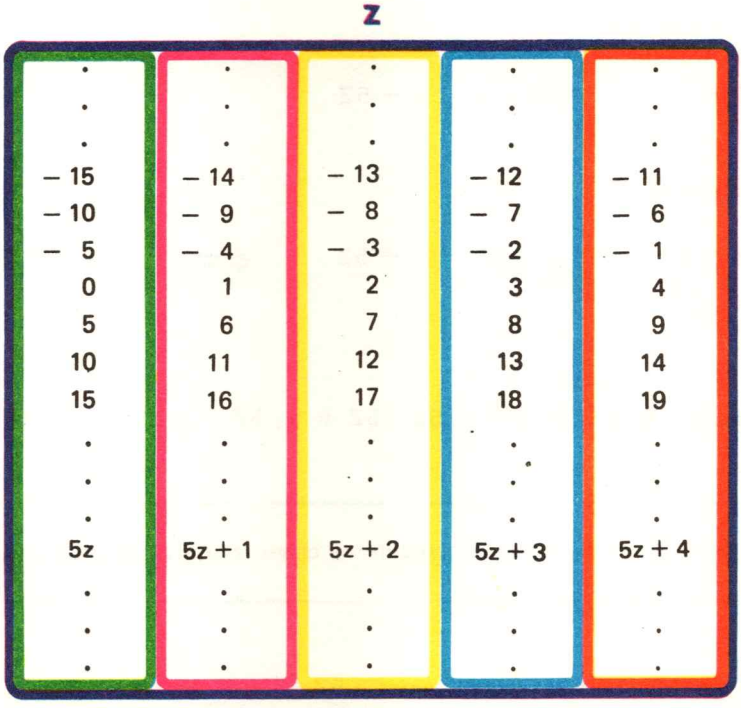
2 – CLASES LATERALES DEL SUBGRUPO 5Z DE Z , +

Recordemos que

$$5\,\mathbf{Z} = \{\, 5z \mid z \in \mathbf{Z} \,\} = \{\, 0, 5, -5, 10, -10, 15, -15, \ldots \text{etc.} \ldots \,\}$$

es un **subgrupo** de **Z**

En el capítulo 7 pusimos en evidencia
la **partición de A definida por el subgrupo 5Z** de **Z , +**



{ 5Z , 5Z + 1 , 5Z + 2 , 5Z + 3 , 5Z + 4 }

ES LA PARTICION DE Z DEFINIDA POR 5Z

FIG. 70

Diremos que $5\mathbb{Z}$, $5\mathbb{Z}+1$, $5\mathbb{Z}+2$,, $5\mathbb{Z}+3$, $5\mathbb{Z}+4$
son las **clases laterales** de $5\mathbb{Z}$

Utilizamos aquí la convención de escritura ya utilizada muchas veces

$$5\mathbb{Z}+1 = \{\, x+1 \;\blacksquare\; x \in 5\mathbb{Z} \,\}$$
$$5\mathbb{Z}+3 = \{\, x+3 \;\blacksquare\; x \in 5\mathbb{Z} \,\}$$

De la misma manera se definiría

$$\forall\, a \in \mathbb{Z} : 5\mathbb{Z}+a = \{\, x+a \;\blacksquare\; x \in 5\mathbb{Z} \,\}$$
$$\forall\, a \in \mathbb{Z} : a+5\mathbb{Z} = \{\, a+x \;\blacksquare\; x \in 5\mathbb{Z} \,\}$$

De donde se concluye

$$\forall\, a \in \mathbb{Z} : \qquad 5\mathbb{Z}+a = a+5\mathbb{Z}$$

Es inmediato que

$$\forall\, a, b \in \mathbb{Z} : \qquad a+5\mathbb{Z} = b+5\mathbb{Z} \iff a-b \in 5\mathbb{Z}$$

Luego

$$\{\, a+5\mathbb{Z} \;\blacksquare\; a \in \mathbb{Z} \,\} = \{\, 5\mathbb{Z} , 5\mathbb{Z}+1 , 5\mathbb{Z}+2 , 5\mathbb{Z}+3 , 5\mathbb{Z}+4 \,\}$$

$\{\, a+5\mathbb{Z} \;\blacksquare\; a \in \mathbb{Z} \,\}$ *es el conjunto de* **clases laterales** *del subgrupo* $5\mathbb{Z}$

Todas las **clases laterales** son equipotentes a $5\mathbb{Z}$

$$\#\, 5\mathbb{Z} = \#\,(1+5\mathbb{Z}) = \#\,(2+5\mathbb{Z}) = \#\,(3+5\mathbb{Z}) = \#\,(4+5\mathbb{Z}) = \delta$$

En el parágrafo siguiente se establecerán resultados análogos para el grupo G , $*$ y uno de sus subgrupos H

3 – CLASES LATERALES DE UN SUBGRUPO DE G , *

DEFINICION

1) Si P *es una parte del grupo* G , * *y* $g \in G$

Entonces

$$g * P = \{ g * p \mid p \in P \}$$
$$P * g = \{ p * g \mid p \in P \}$$

2) Si S *es un subgrupo de* G *y* $g \in G$

Entonces $g * S$ *es la* **clase (lateral) izquierda** *de* S *definida por g*

$S * g$ *es la* **clase (lateral) derecha** *de* S *definida por g*

EJEMPLOS

1. Para todo $n \in \{2, 3, \ldots\}$, el subgrupo $n\mathbf{Z}$ de $\mathbf{Z}$, + admite las n clases laterales

$$n\mathbf{Z} , 1 + n\mathbf{Z} , 2 + n\mathbf{Z} , \ldots , (n - 1) + n\mathbf{Z}$$

Todas estas clases laterales son equipotentes a $n\mathbf{Z}$

El conjunto $\{ z + n\mathbf{Z} \mid z \in \mathbf{Z} \} = \{ n\mathbf{Z} , 1 + n\mathbf{Z} , \ldots , (n - 1) + n\mathbf{Z} \}$ de clases laterales de $n\mathbf{Z}$ es una **partición** *de* $\mathbf{Z}$

2. El conjunto unitario $\{ 0 \}$ es un subgrupo de $\mathbf{Z}$, +

¿Cuáles son las clases laterales de $\{ 0 \}$?

La clase lateral de $\{ 0 \}$ que comprende $z \in \mathbf{Z}$ es

$$z + \{0\} = \{ z + 0 \} = \{ z \}$$

El conjunto de clases laterales de $\{ 0 \}$ es el conjunto de conjuntos unitarios de $\mathbf{Z}$

$$\{ \{ z \} \mid z \in \mathbf{Z} \}$$

Todas las clases laterales de $\{0\}$ son equipotentes a $\{ 0 \}$

El conjunto de clases laterales de $\{0\}$ es una partición de $\mathbf{Z}$

3. $\mathbf{Z}$ es un subgrupo de $\mathbf{Z}$, $+$

$z \in \mathbf{Z}$: $z + \mathbf{Z} = \mathbf{Z} + z = \mathbf{Z}$

De modo que $\mathbf{Z}$ es la única clase lateral de $\mathbf{Z}$

Todas las clases laterales de $\mathbf{Z}$ son equipotentes a $\mathbf{Z}$

El conjunto de clases laterales de $\mathbf{Z}$ es una partición de $\mathbf{Z}$

} ¡Divertido! Pero cierto

4. Si S es un subgrupo del grupo conmutativo G , *

Entonces $\forall\, g \in G$: $g * S = S * g$

Veremos, en el n° 6, que no sucede lo mismo con los grupos no conmutativos.

En un grupo conmutativo,
se puede hablar de **clase lateral**, sin precisar **derecha** o **izquierda.**

5. Ya sabes que el plano punteado Π_0 es un grupo, y que toda recta D_0 que comprende o es un subgrupo de Π_0 , $+$ ([MM1], p. 399 y p. 412)

He aquí $\vec{p} \in \Pi_0$

¿Cuál es la clase lateral de D_0 definida por $\vec{p}$?

Es la paralela a D_0 que comprende $\vec{p}$

El conjunto de clases laterales de D_0 es *dir* D
y es, por lo tanto, una partición de Π_0 en clases equipotentes

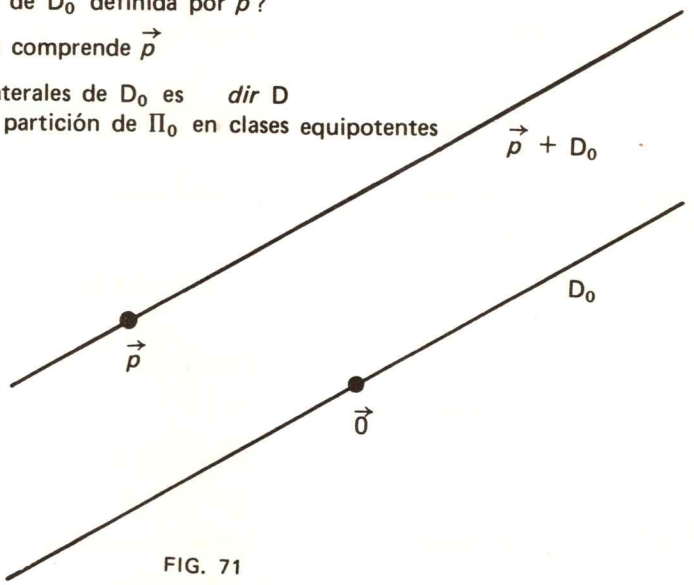
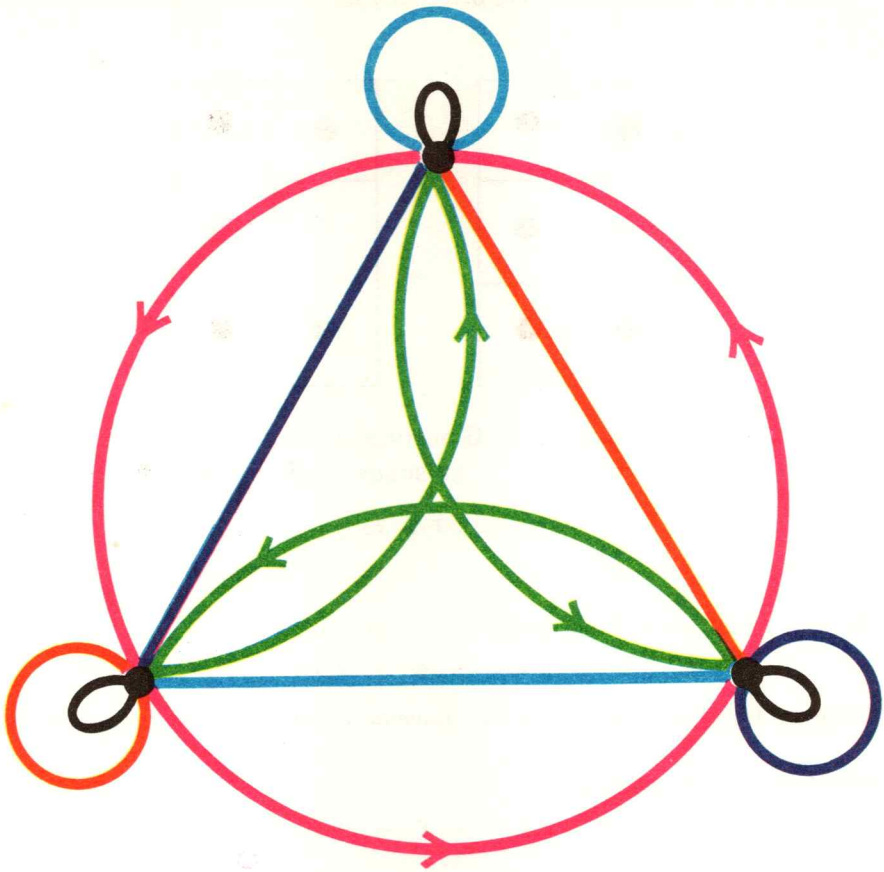


FIG. 71

6. He aquí el grupo G , o de permutaciones de un conjunto que posee tres objetos.

En el esquema figura 72 se representó cada ida y vuelta por un trazo sin flecha.



G = { ● , ● , ● , ● , ● , ● }

FIG. 72

S = { ● , ● } es un subgrupo de G

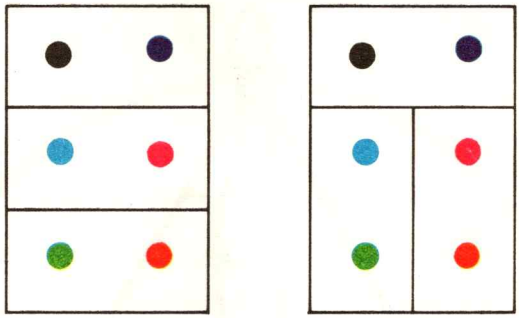
Calculemos la clase izquierda y la clase derecha de S definidas por ●

● o S = ● o { ● , ● } = { ● o ● , ● o ● } = { ● , ● }

S o ● = { ● , ● } o ● = { ● o ● , ● o ● } = { ● , ● }

● o S ≠ S o ●

Determina las tres clases laterales derechas y las tres clases laterales izquierdas de S



LAS DOS PARTICIONES DE **G** DEFINIDAS POR EL SUBGRUPO **S** = { ● ● }

FIG. 73

7. He aquí un subgrupo S del grupo G, $*$ (de neutro ν)

$$\nu * S = S = S * \nu$$

Luego, S es a la vez una clase lateral izquierda y una clase lateral derecha de S

8. Para toda parte P del grupo G, $*$

$$\nu * P = P = P * \nu$$

9. He aquí una parte P del grupo G, $*$ y $a, b \in G$

$$a * (b * P) = \{ a * (b * p) \mid p \in P \}$$
$$= \{ (a * b) * p \mid p \in P \} = (a * b) * P$$

$$\boxed{a * (b * P) = (a * b) * P}$$

PROPOSICION 2

He aquí un subgrupo S *del grupo* G, $*$

Todas las clases laterales de S *son equipotentes a* S

DEMOSTRACION :

Probaremos que la aplicación

$$S \rightarrow g * S \quad : \quad s \rightarrow g * s$$

es una **biyección.**

1°) *La aplicación es suryectiva,* puesto que, por la misma definición

$$g * S = \{ g * s \mid s \in S \}$$

2°) *La aplicación es inyectiva*

Es decir,

$\forall s_1, s_2 \in S :$ $\quad s_1 \neq s_2 \implies g * s_1 \neq g * s_2$

O también,

$\forall s_1, s_2 \in S :$ $\quad g * s_1 = g * s_2 \implies s_1 = s_2$

lo cual es evidente, puesto que

$$g * s_1 = g * s_2 \implies \bar{g} * g * s_1 = \bar{g} * g * s_2 \implies s_1 = s_2$$

Acabamos de establecer que toda clase izquierda de S es equipotente a S

Demostrarás que también toda clase derecha de S es equipotente a S

PROPOSICION 3

Si *g pertenece al subgrupo* S *del grupo* G , *

Entonces $g * S = S = S * g$

Nos limitaremos a establecer la primera igualdad (el lector se encargará de la segunda).

DEMOSTRACION :

1°) $\boxed{g * S \subset S}$

Debemos probar que *todo elemento de* $g * S$ *pertenece a* S

He aquí $x \in g * S$

Luego $x = g * s$ con $s \in S$

($g \in S$ y $s \in S$) implica $g * s \in S$ (puesto que S , * es un grupo).

2°) $\boxed{S \subset g * S}$

Debemos probar que todo elemento de S pertenece a $g * S$

He aquí $s \in S$

$$s = g * \bar{g} * s$$

Como S , * es un subgrupo de G , * :

$$g , s \in S \Longrightarrow \bar{g} , s \in S \Longrightarrow \bar{g} * s \in S$$

Luego $s = g * (\bar{g} * s)$ con $g , \bar{g} * s \in S$

De donde $s \in g * S$

l. q. q. d.

PROPOSICION 4

Si S *es un subgrupo de* G , * *y* $g \in G$

Entonces $g * S = S \iff g \in S \iff S * g = S$

Aquí también nos limitaremos a demostrar la primera de las equivalencias.

La implicación $\Longleftarrow$ acaba de ser demostrada (proposición 3)

DEMOSTRACION DE $\Longrightarrow$

$g * S = S$

Luego, $\forall\, s \in S$: $g * s \in S$

En particular, $g * v \in S$

$g \in S$

l. q. q. d.

TEOREMA 2

He aquí un subgrupo S del grupo G , *

El conjunto de clases izquierdas de S
es una partición de G en clases equipotentes a S

El conjunto de clases derechas de S
es una partición de G en clases equipotentes a S

Sólo nos ocuparemos de las clases izquierdas.

Teniendo en cuenta la proposición 2, sólo falta establecer que el conjunto de clases izquierdas de S es una partición de G

DEMOSTRACION :

1°) Demostraremos primero que

$$\forall g \in G : \qquad g \in g * S$$

En efecto, $\nu \in S$

Por lo tanto $g = g * \nu \in \{ g * s \mid s \in S \} = g * S$

2°) Falta probar que

$\forall g \in G :$ *g pertenece a la única clase* $g * S$

Teniendo en cuenta 1, esto es establecer que

$$\forall g , a \in G : \qquad g \in a * S \implies a * S = g * S$$

En efecto : $g \in a * S \implies g = a * t$ con $t \in S$

$\implies g * S = a * t * S$

$= a * (t * S)$

$= a * S$ (prop. 3)

l. q. q. d.

El teorema 2 y la fórmula $g \in g * S$ implican

LA *clase izquierda de* **S definida por** g (es decir $g * S$)

es

LA *clase izquierda de* S *que comprende* g

4 – ORDEN DE UN GRUPO Y DE SUS SUBGRUPOS

DEFINICION

El orden *de un grupo es el número de elementos que posee.*

Un grupo es **finito ssi** *comprende un número finito de elementos.*

TEOREMA 3

Si S **es un subgrupo del grupo finito** G , *

Entonces el número de clases izquierdas de S **es igual al número de sus clases derechas y se llama índice de** S

Además :

orden de G	=	*orden de* S	•	*índice de* S

En particular :

El orden de todo subgrupo divide el orden del grupo.

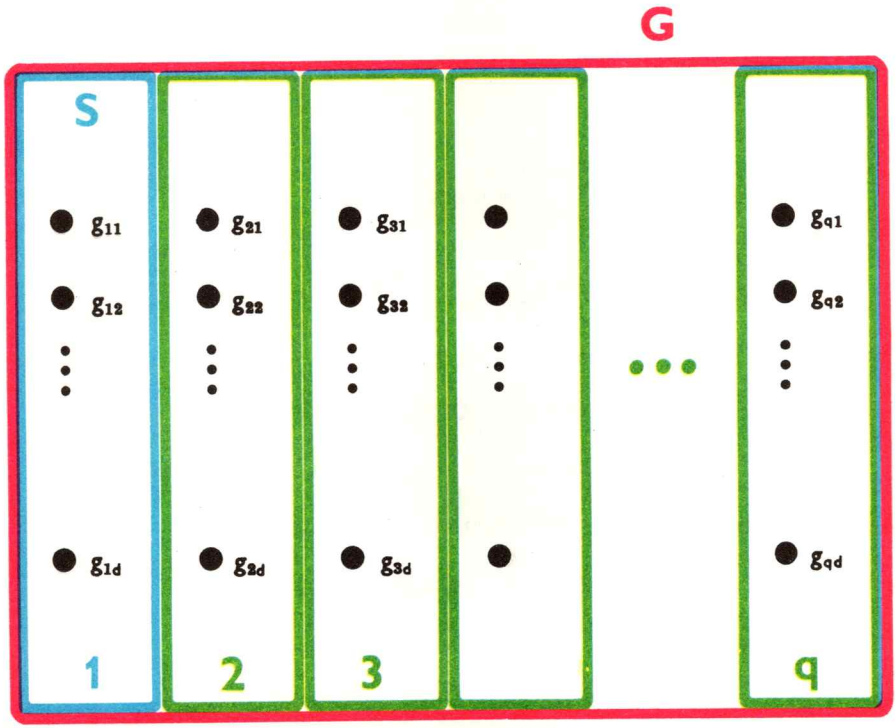
LAGRANGE

DEMOSTRACION :

Sea $d = \#\ S$ y $n = \#\ G$

Sabemos (teorema 2) que el conjunto de clases izquierdas de S es una partición de G en clases tales que cada una comprende d elementos.

Como G es finito, el número de clases izquierdas de G es también un número finito q



PARTICION DEL GRUPO G EN CLASES IZQUIERDAS DE S

FIG. 74

Por lo tanto $n = q\ d$

$q \mid n$

l. q. q. d.

EJERCICIOS

1. Todo grupo $G , *$ admite los subgrupos G y $\{v\}$
   Estos subgrupos se llaman **subgrupos triviales** de $G , *$

2. **Si** El grupo finito $G , *$ es de primer orden
   Entonces los únicos subgrupos de $G , *$ son los subgrupos triviales.

3. Para todo número natural primo p,
   los únicos subgrupos de $Z_p , +$ son sus subgrupos triviales.

4. **Si** S es un subgrupo del grupo $G , *$ y $g, a \in G$
   Entonces
   $$g \in a * S \iff g * S = a * S$$
   $$g \in S * a \iff S * g = S * a$$

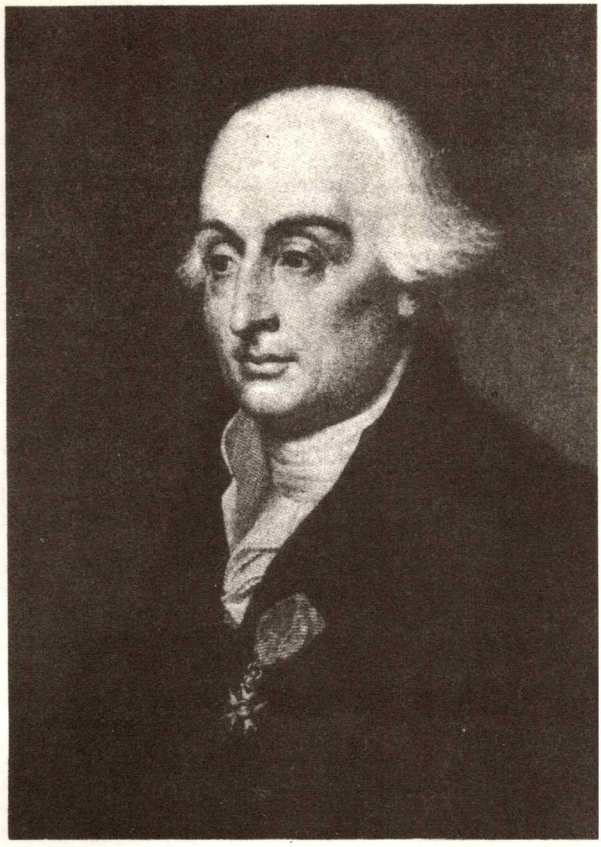
5. **Si** S es un subgrupo del grupo $G , *$ y $g, a \in G$
   Entonces
   $$g \in a * S \iff g * S = a * S$$
   $$\iff a \in g * S$$
   $$\iff \bar{g} * a \in S$$
   $$\iff \bar{a} * g \in S$$

6. Enuncia una proposición análoga a la del ejercicio 5 para las clases derechas.

7. ¿Cuáles son los subgrupos
   del grupo de permutaciones de un conjunto que tiene tres elementos?

8. ¿Cuáles son los subgrupos del grupo $Z_{12} , +$?

LUIS DE LAGRANGE
(nacido en Turín en 1736, muerto en París en 1813)



LAGRANGE nació en Turín el 25 de enero de 1736. Perteneció a una familia emparentada con Descartes. Murió en París el 30 de abril de 1813.

A la edad de 18 años fue nombrado Profesor en la Escuela de artillería de Turín.

A los 23 años Euler le hizo conceder el título de asociado de la Academia de Berlín, de la que fue nombrado Presidente a la edad de 30 años.

Después de la muerte de Federico II, LAGRANGE fue a París, por invitación de Luis XVI.

La obra de LAGRANGE se extiende a todos los dominios de la matemática y de la mecánica de su tiempo.

En 1771, en una memoria consagrada a la resolución de ecuaciones algebraicas, LAGRANGE demuestra, en realidad, el teorema sobre el orden de los subgrupos de los grupos *cíclicos.* También utiliza el teorema general, referente al orden de los subgrupos de grupos cualesquiera, después de haber verificado la validez en algunos ejemplos. En una memoria publicada en 1803, y siempre con motivo de la resolución de ecuaciones algebraicas, otro matemático italiano, ABATTI, demuestra, en realidad, que el orden de todo subgrupo de un grupo finito divide el orden del grupo.

En el momento en que LAGRANGE y ABASTI demostraron estos teoremas, la estructura del grupo no estaba aun esplícitamente tratada. Como no disponían aún del lenguaje de la teoría de grupos, estos autores se expresaban con mucha dificultad y los enunciados están casi siempre colmados de nociones extrañas al tema mismo.

Desde 1682 Leibniz tuvo la intuición del teorema de Wilson, enunciado alrededor de un siglo después, en 1770, por Waring, que lo atribuye a Wilson. La primera demostración conocida se debe a LAGRANGE, en 1771.

* * *

He aquí un extracto de las

SESIONES DE LAS ESCUELAS NORMALES
TOMADAS POR ESTENOGRAFOS
Y REVISADAS POR LOS PROFESORES

DEBATES

Primera sesión (del 11 Pluviôse*)

MATEMATICAS
Lagrange y Laplace, Profesores

Pluviôse. Quinto mes del calendario republicano francés (del 20, 21 ó 22 de enero al 19, 20 ó 21 de febrero).

LAGRANGE – "El día de hoy está destinado a una conferencia sobre la aritmética; pero antes de empezar, haré algunas observaciones sobre esta ciencia. Como no escribí nada al respecto, se las ofreceré en el orden en que se me presenten.

Ustedes deben haber visto, ciudadanos, que la facilidad, la regularidad y la uniformidad de las operaciones aritméticas, se deben a la feliz idea que se tuvo de asignar a cada cifra un valor de posición, haciendo valer diez veces más cada cifra, a medida que se encuentra más hacia la izquierda.

Esta idea tan simple escapó durante mucho tiempo, no sólo a los hombres en general, sino también a los sabios y geómetros. Recién se conoce en Europa a partir del siglo X. El monje francés Gerber la aprendió, al parecer, de los Arabes, que por entonces dominaban a España. Se considera que es el primero que hizo conocer esta idea, como así también las reglas de la aritmética que, naturalemente, dependen de dicha idea. Es por ello que generalmente se atribuye nuestra aritmética a los Arabes.

En general, los antiguos sólo se ocupaban de las propiedades de los números: esas propiedades dan lugar, en efecto, a muchas especulaciones. Hay teorema sobre los números que son muy difíciles de demostrar. Incluso más difíciles que todo lo que se conoce de geometría y álgebra. Por ejemplo, los teoremas concernientes a los números primos.

Se les ha dicho que se llama número primo a los números que no son divisibles por ningún otro número. Así 3, 5, 11, 13 etc. . . son números primos. Lo singular es que, pese a todos los esfuerzos, nunca se pudo encontrar la ley de estos números. Se ha llegado hasta un millón, pero para ello ha sido necesario, cada vez, verificar si el número era divisible por algún otro. Es cierto que cuando se trató de construir tablas, se hallaron medios más fáciles. Actualmente existen tablas de números primos: sobre todo sirven para indicar los números por los cuales se pueden dividir los que no son primos.

A veces resulta útil saber de qué modo un número puede ser producto de la multiplicación de otros números menores; es decir, conocer los factores de un número dado. De ese modo puede reducirse una fracción dada a su más simple expresión, borrando, arriba y abajo de la fracción, los factores comunes. A ello se reduce la regla llamada conjunta en la teoría de cambios.

También se posee tablas de factores de números, pero son poco conocidas, y no se divulgan lo suficiente como para ser de utilidad.

Hasta ahora, no se halló ningún medio de reconocer los números primos a priori, ni de obtener un número primo tan grande como se quiera. Sin embargo, hay algunos interesantes teoremas relativos a esos números. He aquí uno que no presenta ninguna utilidad en la búsqueda de números primos, pero que es admirable por su simplicidad y generalidad.

Si un número es primo, como 5, el producto de todos los números inferiores, 2, 3, 4, más la unidad será divisible por 5. Este producto es 24; agregando la unidad se tiene 25, divisible por 5. Si el número dado es 7, entonces se hará el producto de 2 por 3, por 4, por 5, por 6, que da 720; agregando la unidad se tiene 721, divisible por 7.

Tomemos 11. Se tendrá 2 por 3, por 4, por 5, por 6, por 7, por 8, por 9, por 10, igual a 3.628.800; agregando la unidad se tiene 3.628.801, divisible por 11, siendo el cociente 329.891.

Este teorema es uno de los más hermosos que se haya encontrado hasta ahora. Es sobre todo admirable, porque se verifica cada vez que se tome un número primo, pero no se verifica si el número no es primo. Esto es fácil de comprobar.

* * *

Tomamos este extracto de un muy buen libro de Pierre DEDRON y Jean ITARD, Matemática y Matemáticos*. Puede ser que este pasaje te incite a leer ese libro, que debería figurar en todas las bibliotecas escolares.

(1) MAGNARD, Paris, 1959.

11

Orden de los elementos de un grupo

G , · es un grupo cuyo neutro se anota 1

El inverso o simétrico del elemento g de G se anota g^{-1}

1 – POTENCIAS EN UN GRUPO MULTIPLICATIVO

En el capítulo 8, introdujimos las potencias (con exponentes enteros racionales) en los grupos multiplicativos de cuerpos. Esta teoría sigue siendo válida en todo grupo multiplicativo.

DEFINICION

Si *g es un elemento del grupo* G , · y $n \in \omega_0$

Entonces $g^n = \underbrace{g \cdot \ldots \cdot g}_{n \text{ factores}}$ $\qquad g^0 = 1$

De donde resulta, inmediatamente, que :

Si *g es un elemento del grupo* G , · y $n \in \omega_0$

Entonces $g^n \cdot (g^{-1})^n = 1 = (g^{-1})^n \cdot g^n$

Luego

$$(g^n)^{-1} = (g^{-1})^n$$

Esta fórmula introduce la definición de potencias con exponentes enteros racionales de los elementos del grupo $G, \cdot$

DEFINICION

Si $g \in G, \cdot$ y $m \in \omega_0$

Entonces $g^m = \underbrace{g \cdot \ldots \cdot g}_{m \text{ factores}}$; $g^0 = 1$; $g^{-m} = (g^{-1})^m = (g^m)^{-1}$

Se concluye fácilmente

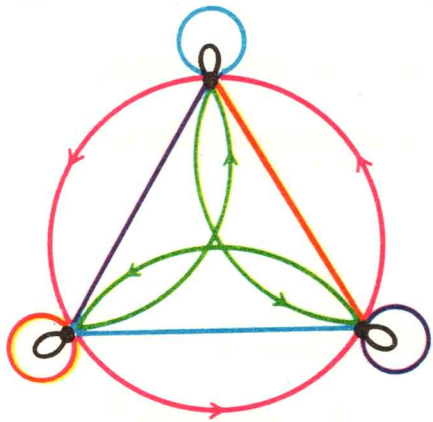
Si g es un elemento del grupo $G, \cdot$ y $a, b \in \mathbf{Z}$

Entonces $g^a \cdot g^b = g^{a+b}$ y $(g^a)^b = g^{ab}$

Estas fórmulas generalizan los resultados del capítulo 8, § 1, para los grupos multiplicativos de cuerpos.

Sin embargo, cuidémonos de extraer conclusiones prematuras.

¡ATENCION!



$G = \{ \bullet, \bullet, \bullet, \bullet, \bullet, \bullet \}$

Las potencias en G, $\circ$ se definen considerando $\circ$ como $\cdot$

$(\bullet \circ \bullet)^2 = \bullet^2 = \bullet$

$\bullet^2 \circ \bullet^2 = \bullet \circ \bullet = \bullet$

$(\bullet \circ \bullet)^2 \neq \bullet^2 \circ \bullet^2$

EJEMPLOS

G , · *es un grupo*

1. Si $g, h \in G, \cdot$

Entonces $(g \cdot h)^{-1} = h^{-1} \cdot a^{-1}$

2. Si $g, h, k \in G, \cdot$

Entonces $(g \cdot h \cdot k)^{-1} = k^{-1} \cdot h^{-1} \cdot g^{-1}$

3. Si $g, h, \ldots, k$ designan un número finito de elementos de G ,

Entonces $(g \cdot h \cdot \ldots \cdot k)^{-1} = k^{-1} \cdot \ldots \cdot h^{-1} \cdot g^{-1}$

4. Si $g, h \in G, \cdot$ y $g \cdot h = h \cdot g$

Entonces

$$\begin{aligned}(gh)^2 &= gh \cdot gh \\ &= g \cdot hg \cdot h \\ &= g \cdot gh \cdot h \\ &= gg \cdot hh = g^2 \cdot h^2\end{aligned}$$

$$\begin{aligned}(gh)^3 &= gh \cdot gh \cdot gh \\ &= g \cdot hg \cdot hg \cdot h \\ &= g \cdot gh \cdot gh \cdot h \\ &= gg \cdot hg \cdot hh \\ &= gg \cdot gh \cdot hh \\ &= ggg \cdot hhh = g^3 \cdot h^3\end{aligned}$$

¡Salta conejito!
¡Salta conejito!
¡Salta, salta, conejín!

5. **Si** $g, h \in G, \cdot$ y $gh = hg$

Entonces $\forall\ n \in \omega :\quad (g \cdot h)^n = g^n \cdot h^n = h^n \cdot g^n$

Luego

$$\begin{aligned}(gh)^{-n} &= ((g\,h)^n)^{-1}\\ &= (h^n\,g^n)^{-1}\\ &= (g^n)^{-1} \cdot (h^n)^{-1} = g^{-n} \cdot h^{-n}\end{aligned}$$

Si *g, h son elementos del grupo* $G, \cdot$ *y* $gh = hg$

Entonces $\forall\ z \in \mathbf{Z} :\qquad (gh)^z = g^z \cdot h^z$

6. La fórmula

$$\forall\, g \in G\ ;\ \forall\, a, b \in \mathbf{Z} :\quad (g^a)^b = g^{ab} = (g^b)^a$$

implica

$$\forall\, g \in G\ ;\ \forall z \in \mathbf{Z} :\quad (g^{-1})^z = g^{-z} = (g^z)^{-1}$$

7. $\forall\, g \in G\ ;\ \forall\, a, b \in \mathbf{Z} :\quad g^a = g^b \iff g^{a-b} = 1$

8. $\forall\, g \in G\ ;\ \forall\, a, b \in \mathbf{Z} :\quad g^a \neq g^b \iff g^{a-b} \neq 1$

2 – SUBGRUPO ENGENDRADO POR UN ELEMENTO

He aquí un elemento g del grupo $G, \cdot$

y el conjunto de sus potencias (con exponentes enteros racionales)

$$\{ g^z \mid z \in \mathbf{Z} \} = \{ \ldots, g^{-3}, g^{-2}, g^{-1}, g^0 = 1, g = g^1, g^2, \ldots \}$$

Todo subgrupo de $G, \cdot$ que comprende g, comprende también

$$1 = g^0$$

$$g = g^1 \ , \quad g \cdot g = g^2 \ , \quad g \cdot g^2 = g^3 \ , \ \ldots$$

$$g^{-1} \ , \ g^{-1} \cdot g^{-1} = g^{-2} \ , \ g^{-1} \cdot g^{-2} = g^{-3} \ , \ \ldots$$

Luego todo subgrupo de $G, \cdot$ que comprende g contiene $\{ g^z \mid z \in \mathbf{Z} \}$

Pero $\{ g^z \mid z \in \mathbf{Z} \}$ es un subgrupo de $G, \cdot$ porque

$$1^\circ) \ g^a \cdot g^b = g^{a+b}$$

$$2^\circ) \ g^0 = 1$$

$$3^\circ) \ g^a \cdot g^{-a} = 1$$

Acabamos de establecer el

TEOREMA 1

Si g **es un elemento del grupo** $G, \cdot$

Entonces $\{ g^z \mid z \in \mathbf{Z} \}$ **es el menor subgrupo de** $G, \cdot$ **que comprende** g

Se le llama subgrupo de $G, \cdot$ **engendrado por** g

y se anota $\operatorname{grp} g$

$$\operatorname{grp} g = \{ g^z \mid z \in \mathbf{Z} \}$$

* * *

El grupo $G, \cdot$ se anota multiplicativamente por pura convención de escritura.

Los resultados obtenidos pueden ser expresados en anotación aditiva. Se generaliza así lo que vimos en el capítulo 2 para el grupo $\mathbf{Z}, +$

Pequeño Diccionario

Grupo multiplicativo	*Grupo aditivo*
G	G , +
unidad	cero
1	0
inverso	opuesto
$g \in G$	$g \in G$
g^{-1}	$-g$
$g \cdot g = g^2$	$g + g = 2g$
g^n	ng
$(g^{-1})^n = (g^n)^{-1}$	$n(-g) = -(ng)$
$g^{-n} = (g^{-1})^n = (g^n)^{-1}$	$(-n)g = n(-g) = -(ng)$
grp	*mod*
grp g	*mod* g
grp $g = \{ g^z \mid z \in \mathbf{Z} \}$	*mod* $g = \{ zg \mid z \in \mathbf{Z} \}$

TEOREMA 1

Si g **es un elemento del grupo** $G , +$

Entonces $Zg = \{ zg \mid z \in Z \}$

es el menor subgrupo de $G , +$ **que comprende** g

Se le llama subgrupo (o módulo) de $G , +$ **engendrado por** g

y se lo anota *mod* g

Versión aditiva

$$mod\ g = Z\ g = \{ z\ g \mid z \in Z \}$$

DEFINICION

Un grupo es cíclico **ssi** *está engendrado por uno de sus elementos.*

El subgrupo S del grupo $G , \cdot$ es cíclico	El subgrupo S del grupo $G , +$ es cíclico
ssi	**ssi**
$\exists g \in G : S = grp\ g$	$\exists g \in G : S = mod\ g$

Esta definición permite volver a formular la proposición 5 del capítulo 2.

Todos los subgrupos de $Z , +$ **son cíclicos.**

EJEMPLOS

1. En $Q_0 , \cdot$: $\quad \text{grp } 2 = \{ 2^z \mid z \in \mathbf{Z} \} \quad ; \quad \# \text{ grp } 2 = \delta$

$$\text{grp } 1 = \{ 1 \} \quad ; \quad \# \text{ grp } 1 = 1$$

$$\text{grp } (-1) = \{ 1, -1 \} \quad ; \quad \# \text{ grp } (-1) = 2$$

2. En todo grupo $G , \cdot$ (cuyo neutro se anota 1)

$$\text{grp } 1 = \{ 1 \} \quad ; \quad \# \text{ grp } 1 = 1$$

$$\forall g \in G , \cdot \; : \; \# \text{ grp } g = 1 \iff g = 1$$

(En la última fórmula, el segundo 1 es el neutro de $G , \cdot$ y el primer 1 es el número natural 1)

3. En todo grupo $G , +$ (cuyo neutro se anota 0)

$$mod\ 0 = \{ 0 \} \quad ; \quad \# mod\ 0 = 1$$

$$\forall g \in G , + \; : \; \# mod\ g = 1 \iff g = 0 .$$

(En la última fórmula, 1 designa el número natural 1 y 0 el neutro de $G , +$)

4. $\mathbf{Z} , +$ y sus subgrupos son grupos cíclicos isomorfos.

5. $\mathbf{Z} , + ; \; \mathbf{Z}_2 , + ; \; \mathbf{Z}_3 , + ; \; \mathbf{Z}_4 , + ; \; \ldots ; \; \mathbf{Z}_n , + ; \; \ldots$

son grupos cíclicos no isomorfos.

Después se verá que todo grupo cíclico es isomorfo a $\mathbf{Z} , +$ o a uno de los $\mathbf{Z}_n , +$

6. Si g es un elemento del grupo $G , \cdot$

Entonces $\# \text{ grp } g = \delta$ **o** $\# \text{ grp } g \in \omega_0$

7. Si g es un elemento del grupo finito G , $\cdot$

Entonces grp g es un grupo cíclico de G , $\cdot$

Luego $\#\ \text{grp}\ g \mid \#\ G$

8. Si g es un elemento del grupo G , $\cdot$

Entonces grp g es un grupo cíclico y $\text{grp}\ g^{-1} = \text{grp}\ g$

9. Expresa el n° 8 en la anotación aditiva.

10. Todo grupo de primer orden es cíclico.

multiplicación	adición
producto	suma
potencia	múltiplo
exponente	coeficiente
g^z	zg

FRAGMENTO DEL "PEQUEÑO DIDIER"

FIG. 75

3 – ORDEN DE UN ELEMENTO DE UN GRUPO

DEFINICION

El orden de un elemento *de un grupo es el orden del subgrupo que él engendra. El orden del elemento g se anota* $\sigma(g)$

$$\forall g \in G, \cdot : \sigma(g) = \# \text{ grp } g$$

El orden de un elemento de un grupo es, por consiguiente, un natural no nulo o δ

EJEMPLOS

1. **Si** g es un elemento del grupo $G, \cdot$

   Entonces $\sigma(g) = \# \text{ grp } g$

   $\sigma(g) = 1 \iff g = 1$

2. **Si** g es un elemento del grupo $G, +$

   Entonces $\sigma(g) = \# \text{ mod } g$

   $\sigma(g) = 1 \iff g = 0$

3. En $Q_0, \cdot$ $\quad \sigma(2) = 0 \quad ; \quad \sigma(1) = 1 \quad ; \quad \sigma(-1) = 2$

4. Para todo elemento g del grupo $G, \cdot$ $\quad \sigma(g^{-1}) = \sigma(g)$

5. Expresión del nº 4 en la notación aditiva.

6. Si g es un elemento del grupo finito G, $\cdot$

Entonces grp g es un subgrupo de G, $\cdot$

y $\sigma(g) = \#\ \text{grp}\ g \mid \#\ G$ (Lagrange)

El orden de un elemento de un grupo finito divide el orden del grupo

* * *

He aquí el subgrupo grp g engendrado por el elemento g del grupo G, $\cdot$

$$\text{grp}\ g = \{ \ldots, g^a, \ldots, g^b, \ldots \}$$

Se da una de estas dos cosas :

o bien

1

$\forall a, b \in \mathbf{Z}$:

$a < b \iff g^a \neq g^b$

o bien

2

$\exists\ a, b \in \mathbf{Z}$:

$a < b$ y $g^a = g^b$

Examinemos sucesivamente estas dos eventualidades

1

$\mathbf{Z} \to \text{grp}\ g : z \to g^z$ es una biyección

$$\sigma(g) = \#\ \text{grp}\ g = \#\ \mathbf{Z} = \delta$$

Por la biyección indicada

$$a \to g^a$$
$$b \to g^b$$
$$a + b \to g^{a+b} = g^a \cdot g^b$$

Esta biyección es, pues, un isomorfismo
del grupo aditivo $\mathbf{Z}$, $+$ sobre el grupo multiplicativo grp g , $\cdot$

$$\forall\, n \in \omega_0 \qquad g^n \neq 1$$
$$\text{grp } g \text{ , } \cdot \quad \textit{isomorfo a} \quad \mathbf{Z} \text{ , } +$$

2

He aquí $a, b \in \mathbf{Z}$ tales que $a < b$ y $g^a = g^b$

Luego $b - a > 0$ y $g^{b-a} = 1$

El número $b - a$ es un natural no nulo tal que $g^{b-a} = 1$

Llamemos n al menor natural no nulo tal que $g^n = 1$

Examinemos $\{ g = g^1 , g^2 , \ldots , g^{n-1} , g^n = 1 \}$

Probemos que los n términos $g^1, g^2, \ldots, g^{n-1}, g^n$ son distintos.

Si $1 \leqslant c < d \leqslant n$

Entonces $g^d \cdot (g^c)^{-1} = g^d \cdot g^{-c} = g^{d-c}$ con $d - c < n$

Como n es el menor número natural no nulo tal que $g^n = 1$

$$g^d \cdot g^{-c} \neq 1 \quad \text{de donde} \quad g^c \neq g^d .$$

los n términos $g^1, g^2, \ldots, g^{n-1}, g^n$ son distintos

y $\# \{ g = g^1 , g^2 , \ldots , g^{n-1} , g^n = 1 \} = n$

Pero

$$\begin{array}{l|l|l|l|l}
g^1 = g^{n+1} & g^2 = g^{n+2} & \cdots & g^{n-1} = g^{n+n-1} & g^n = g^{2n} \\
\quad = g^{2n+1} & \quad = g^{2n+2} & \cdots & \quad = g^{2n+n-1} & \quad = g^{3n} \\
\quad = & & & & \\
\quad \vdots & & & & \\
\quad = g^{-n+1} & \quad = g^{-n+2} & \cdots & \quad = g^{-n+n-1} & \quad = g^0 \\
\quad = g^{-2n+1} & \quad = g^{-2n+2} & \cdots & \quad = g^{-2n+n-1} & \quad = g^{-n} \\
\quad = & & & & \\
\quad \vdots & & & &
\end{array}$$

Luego $\operatorname{grp} g = \{ g = g^1 , g^2 , \ldots , g^{n-1} , g^n = 1 \}$

$\sigma(g) = \# \operatorname{grp} g = n$

y $$\boxed{\forall\, m \in \mathbf{Z} \quad : \quad g^m = 1 \iff \sigma(g) \mid m} \qquad (1)$$

Para todo $a, b \in \mathbf{Z}$:

$$g^a = g^b \iff g^{b-a} = 1 \iff n \mid (b-a) \iff \bar{a} = \bar{b}$$

donde $\bar{a}, \bar{b} \in \mathbf{Z}_n$

$$\boxed{g^a = g^b \iff \bar{a} = \bar{b}}$$

Así

$$\begin{array}{rcl}
\to \operatorname{grp} g \ : \ \bar{x} & \to & g^x \\
\bar{a} & \to & g^a \\
\bar{b} & \to & g^b \\
\bar{a} + \bar{b} = \overline{a+b} & \to & g^{a+b} = g^a \cdot g^b
\end{array}$$

es una biyección tal que

es decir, es un isomorfismo del grupo $\mathbf{Z}_n$, $+$ sobre el grupo $\operatorname{grp} g$, $\cdot$

$n = \sigma(g)$ *es el menor número natural no nulo tal que* $g^n = 1$

grp g , $\cdot$ *es isomorfo a* $\mathbf{Z}_n$, $+$

Si G es un grupo finito de orden k

Entonces $\sigma(g) \mid k$ y en virtud de (1) : $g^k = 1$

De esta manera, hemos establecido el

TEOREMA 2

He aquí un elemento g del grupo G , $\cdot$ y $m \in \mathbf{Z}$

$\sigma(g) = \delta$	$\sigma(g) = n \in \omega_0$
$\Updownarrow$	$\Updownarrow$
$\forall n \in \omega_0 : \quad g^n \neq 1$	n **es el menor número natural no nulo tal que** $g^n = 1$
$\Updownarrow$	$\Updownarrow$
grp g , $\cdot$ **isomorfo a** $\mathbf{Z}$, $+$	grp g , $\cdot$ **isomorfo a** $\mathbf{Z}_n$, $+$

Si g **es de orden finito** **Entonces** $g^m = 1 \iff \sigma(g) \mid m$

Si G **es de orden finito** k **Entonces** $g^k = 1$

Si el grupo G , $\cdot$ es cíclico,

Entonces G , $\cdot$ = grp g, $\cdot$ con $g \in$ G

G , $\cdot$ es isomorfo a $\mathbf{Z}$, $+$ o a uno de los $\mathbf{Z}_n$, $+$ (Teorema 2)

Todo grupo cíclico es isomorfo a $\mathbf{Z}$, $+$ **o a uno de los** $\mathbf{Z}_n$, $+$

(*con* $n \in \omega_0$)

EJERCICIOS

1. Todo grupo cíclico es conmutativo.
2. Un grupo finito G es cíclico (es decir, está engendrado por uno de sus elementos)

ssi

G comprende (por lo menos) un elemento tal que $o(g) = \# G$

3. ¿Cuáles son los órdenes de los elementos del grupo de simetrías centrales y traslaciones del plano Π?
4. ¿Cuáles son los órdenes de los elementos del grupo simétrico de $\{1, 2, 3\}$
5. ¿Cuáles son los órdenes de los elementos del grupo de permutaciones de un conjunto de cuatro elementos?

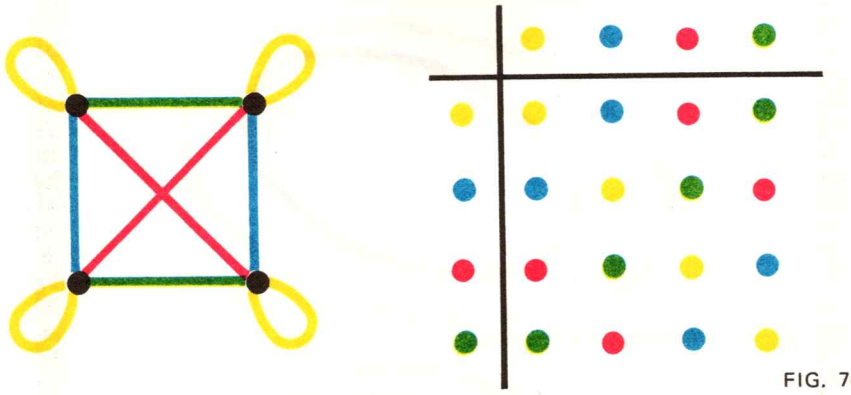


FIG. 76

GRUPO DE PERMUTACIONES DE UN CONJUNTO DE CUATRO ELEMENTOS

6. **Si** g es un elemento de orden finito del grupo $M , +$

   Entonces el orden de g es el menor número natural no nulo a tal que $ag = 0$

7. El grupo $R , +$ no es cíclico.
8. El grupo $Q , +$ no es cíclico.
9. El grupo de permutaciones de un conjunto de cuatro elementos no es cíclico.
10. $Q_0 , \cdot$ no es cíclico.
11. $R_0 , \cdot$ no es cíclico.
12. La fórmula de Fermat es una consecuencia inmediata del teorema 2

4 – POTENCIAS DE ELEMENTOS DE ORDEN FINITO DE UN GRUPO

Si g es un elemento de orden finito del grupo $G, \cdot$ y $m \in \mathbf{Z}$

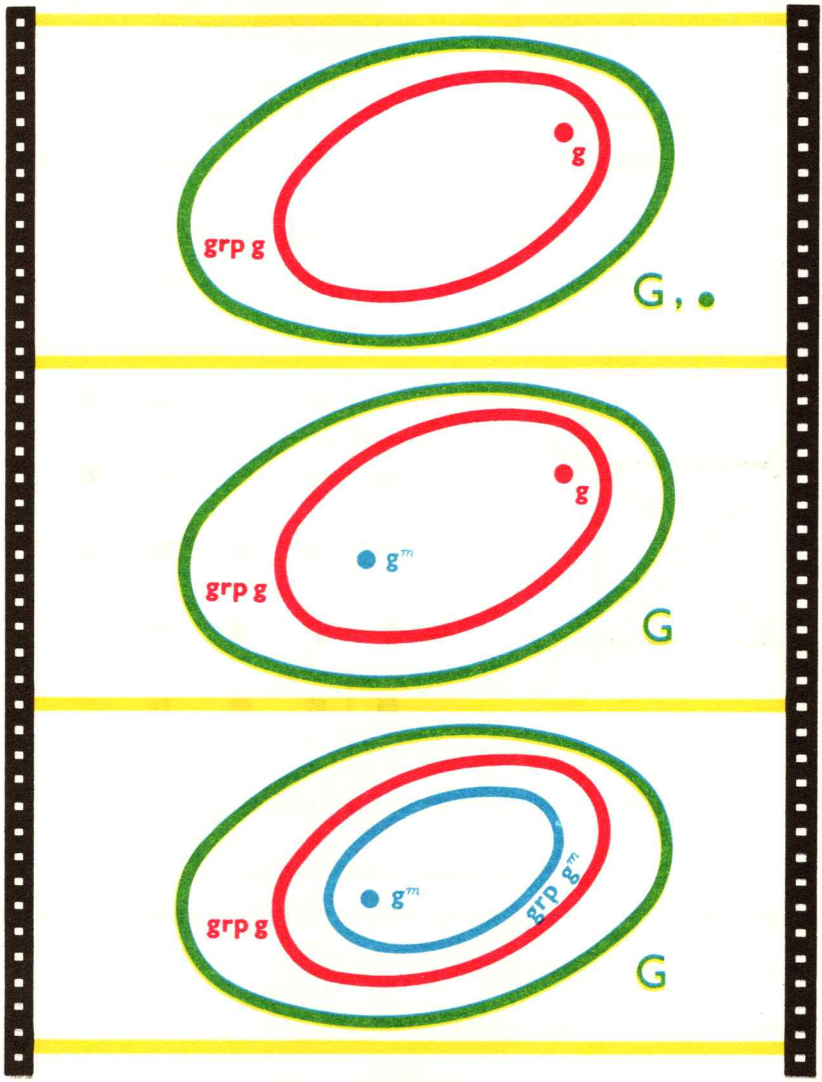


FIG. 77

Entonces grp g^m es un subgrupo de grp g

de donde $\sigma(g^m) \mid \#\,\text{grp}\ g = \sigma(g)$

y $\text{grp}\ g^m = \text{grp}\ g \iff \sigma(g^m) = \sigma(g)$

TEOREMA 3

Si g **es un elemento de orden finito del gupo** $G, \cdot$ **y** $m \in \mathbf{Z}$

Entonces

$$\sigma(g^m) = \frac{\sigma(g)}{m \wedge \sigma(g)}$$

En particular

1°) **Si** $m \mid \sigma(g)$ **Entonces** $\sigma(g^m) = \sigma(g) / m$

2°) grp g = grp g^m $\iff$ $\sigma(g) = \sigma(g^m)$ $\iff$ $m \wedge \sigma(g) = 1$

Sea $\sigma(g) = n$

En virtud del teorema 2

n es el menor número natural no nulo tal que $g^n = 1$ (1)

Demostración del caso particular 1

1°) $m \mid n$ **luego** $\frac{n}{m} \in \mathbf{Z}$ y $(g^m)^{\frac{n}{m}} = g^n = 1$

$$(g^m)^{\frac{n}{m}} = 1$$

$$\sigma(g^m) \mid \frac{n}{m}$$ (Teorema 2)

$$\sigma(g^m) \leqslant \frac{n}{m}$$

2°) Si $k < \frac{n}{m}$ (con $k \in \omega_0$)

Entonces $mk < n$

$g^{mk} \neq 1$ (en virtud de (1))

$(g^m)^k \neq 1$

3°) $\frac{n}{m}$ es, por consiguiente, el menor número natural no nulo tal que

$$(g^m)^{\frac{n}{m}} = 1$$

de donde $\sigma(g^m) = \frac{n}{m}$ (Teorema 2)

es decir $\sigma(g^m) = \frac{\sigma(g)}{m}$

l. q. q. d.

Demostración del teorema propiamente dicho.

Sea $d = m \wedge n$

$d = m' m + n' n$ (con $m', n' \in \mathbf{Z}$)

$$g^d = g^{m'm+n'n} = g^{m'm} \cdot g^{n'n} = (g^m)^{m'} \cdot (g^n)^{n'} = (g^m)^{m'} \cdot 1^{n'} = (g^m)^{m'}$$

$$\boxed{g^d = (g^m)^{m'} \cdot}$$

$d \mid m \Longrightarrow g^m \in \operatorname{grp} g^d \Longrightarrow \operatorname{grp} g^m \subset \operatorname{grp} g^d$

$g^d = (g^m)^{m'} \Longrightarrow g^d \in \operatorname{grp} g^m \Longrightarrow \operatorname{grp} g^d \subset \operatorname{grp} g^m$

Luego

$$\operatorname{grp} g^m = \operatorname{grp} g^d$$
$$\sigma(g^m) = \sigma(g^d) \qquad (2)$$

Como $d \mid m$, podemos calcular $\sigma(g^d)$ aplicando el caso particular 1

$$\sigma(g^d) = \frac{n}{d} = \frac{n}{m \wedge n}$$

$$\sigma(g^d) = \frac{\sigma(g)}{m \wedge \sigma(g)} \qquad (3)$$

Las fórmulas (2) y (3) implican

$$\sigma(g^m) = \frac{\sigma(g)}{m \wedge \sigma(g)}$$

l. q. q. d.

El primer caso particular del teorema 3 muestra que

Si el número natural d divide el orden finito de un elemento del grupo $G, \cdot$

Entonces existe por lo menos un elemento del grupo $G, \cdot$ cuyo orden es d

EJERCICIOS

1. Expresa el teorema 3 en notación aditiva.

2. Calcula el orden de los elementos de $\mathbf{Z}_{12}$, $+$

3. En $\mathbf{Z}_{12}$, $+$

$$\sigma(\overline{m}) = \sigma(m \cdot \overline{1}) = \frac{\sigma(\overline{1})}{m \wedge \sigma(\overline{1})} = \frac{12}{m \wedge 12}$$

4. En $\mathbf{Z}_n$, $+$ $\qquad \sigma(\overline{m}) = \dfrac{n}{m \wedge n}$

5.

	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{12}$	$\overline{13}$	$\overline{14}$
Z_2	1	2													
Z_3	1	3	3												
Z_4	1	4	2	4											
Z_5	1	5	5	5	5										
Z_6	1	6	3	2	3	6									
Z_7	1	7	7	7	7	7	7								
Z_8	1	8	4	8	2	8	4	8							
Z_9	1	9	9	3	9	9	3	9	9						
Z_{10}	1	10	5	10	5	2	5	10	5	10					
Z_{11}	1	11	11	11	11	11	11	11	11	11	11				
Z_{12}	1	12	6	4	3	12	2	12	3	4	6	12			
Z_{13}	1	13	13	13	13	13	13	13	13	13	13	13	13		
Z_{14}	1	14	7	14	7	14	7	2	7	14	7	14	7	14	
Z_{15}	1	15	15	5	15	3	5	15	15	5	3	15	5	15	15

ORDEN DEL ELEMENTO $\overline{m}$ EN EL GRUPO Z_n , +

FIG. 78

5 – ORDEN Y PRODUCTO

PROPOSICION 1

Si *g, h son elementos de orden finito del grupo* G , · *tales que*
$gh = hg$ *y* $o(g) \wedge o(h) = 1$

Entonces $o(gh) = o(g) \cdot o(h)$

DEMOSTRACION :

Sea $a = gh$, $m = o(g)$, $n = o(h)$, $d = o(a)$

Se debe probar que $d = mn$

1°) $a^{mn} = (gh)^{mn} = g^{mn} \cdot h^{mn} = (g^m)^n \cdot (h^n)^m = 1^n \cdot 1^m = 1$

Luego $\boxed{d \mid mn}$ (1)

2°) $a^n = (gh)^n = g^n h^n = g^n \cdot 1 = g^n$ (2)

Como $m \wedge n = 1$ el teorema 3 nos enseña que

$$o(g^n) = o(g)$$

De donde se obtiene, sucesivamente

$$\begin{aligned} \text{grp } g^n &= \text{grp } g \\ g &\in \text{grp } g^n \\ g &= (g^n)^t \qquad (\text{con } t \in \mathbf{Z}) \\ g &= (a^n)^t = a^{nt} \qquad (\text{en virtud de la fórmula (2)}) \\ g^d &= (a^d)^{nt} = 1^{nt} = 1 \\ m &= o(g) \mid d \qquad (\text{teorema 2}) \end{aligned}$$

También $n \mid d$

Pero $m \mid d$, $n \mid d$, $m \wedge n = 1 \implies mn \mid d$

Luego $\boxed{\text{mn} \mid \text{d}}$ (3)

Las fórmulas (1) y (3) implican

$$\boxed{mn = d}$$

l. q. q. d.

PROPOSICION 2

Si *los elementos* $g_1, \ldots, g_k$ *pertenecen al grupo* **conmutativo** $G, \cdot$

Entonces *el grupo* $G, \cdot$ *comprende por lo menos un elemento* g *de orden*

$$\sigma(g) = \sigma(g_1) \vee \ldots \vee \sigma(g_k)$$

DEMOSTRACION :

Llamemos $p_1, \ldots, p_t$ a los números primos distintos que aparecen en las factorizaciones primas de los órdenes $\sigma(g_1), \ldots, \sigma(g_k)$

Para todo $i \in \{1, \ldots, t\}$ designemos con m_i el mayor exponente que afecta a p_i en estas factorizaciones.

Así $$\sigma(g_1) \vee \ldots \vee \sigma(g_k) = {p_1}^{m_1} \cdot \ldots \cdot {p_t}^{m_t}$$

Como ${p_i}^{m_i}$ divide el orden de uno (por lo menos) de los $g_1, \ldots, g_k$ sabemos (en virtud del teorema 3) que seguramente existe un $h_i \in G$ tal que $\sigma(h_i) = {p_i}^{m_i}$

$$\sigma(h_1) \wedge \sigma(h_2) = {p_1}^{m_1} \wedge {p_2}^{m_2} = 1 \quad \text{y} \quad h_1 \cdot h_2 = h_2 \cdot h_1$$

Luego (prop. 6)

$$\sigma(h_1 \cdot h_2) = \sigma(h_1) \cdot \sigma(h_2) = {p_1}^{m_1} \cdot {p_2}^{m_2}$$

$$\sigma(h_1 h_2) \wedge \sigma(h_3) = {p_1}^{m_1} {p_2}^{m_2} \wedge {p_3}^{m_3} = 1 \quad \text{y} \quad h_1 h_2 \cdot h_3 = h_3 \cdot h_1 h_2$$

Luego (prop. 6)

$$\sigma(h_1 h_2 h_3) = \sigma(h_1 h_2) \cdot \sigma(h_3) = {p_1}^{m_1} {p_2}^{m_2} {p_3}^{m_3}$$

etc.

Finalmente,

$$\sigma(h_1 h_2 \ldots h_t) = {p_1}^{m_1} {p_2}^{m_2} \ldots {p_t}^{m_t} = \sigma(g_1) \vee \ldots \vee \sigma(g_k)$$

l. q. q. d.

EJERCICIOS

1. **Si** $f : G, \cdot \rightarrow H, \cdot$ es un isomorfismo de grupos

Entonces $\forall\, x \in G : \quad \sigma(x) = \sigma(f(x))$

2. Todos los elementos del grupo de permutaciones de un conjunto de cuatro elementos son de orden 1 o 2

Dicho grupo no es isomorfo a $\mathbf{Z}_4$

3. En un grupo $G, \cdot$

Si a, b son de orden finito y $ab = ba$

Entonces $ab = ba$ es de orden finito.

4. En el grupo $G, \cdot$ de traslaciones y simetrías centrales del plano Π

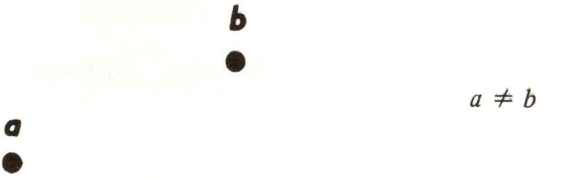


FIG. 79

$$s_b \circ s_a = \overrightarrow{2ab} \neq \overrightarrow{2ba} = s_a \circ s_b$$

$$\sigma(s_a) = 2 = \sigma(s_b)$$

$$\sigma(s_a \circ s_b) = \sigma(\overrightarrow{2ba}) = \delta$$

$$\sigma(s_b \circ s_a) = \sigma(\overrightarrow{2ab}) = \delta$$

5. **Si** a, b son elementos de orden finito del grupo $G, \cdot$ tales que $ab = ba$

Entonces $\sigma(ab) \mid \sigma(a) \vee \sigma(b)$

6. En el grupo de permutaciones de tres objetos

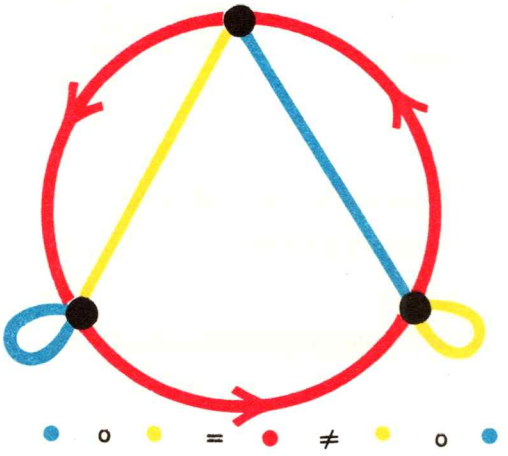


FIG. 80

$\sigma(\bullet) = \sigma(\bullet) = 2 \qquad \sigma(\bullet \circ \bullet) = \sigma(\bullet) = 3$

$3 \nmid 2 \vee 2$

7. Volvamos a formular la

Proposición 1

Si g, h son elementos de orden finito del grupo $G, \cdot$ tales que $gh = hg$

Entonces $\sigma(g) \wedge \sigma(h) = 1 \implies \sigma(gh) = \sigma(g) \vee \sigma(h)$

Cuidémonos, sin embargo, de generalizaciones prematuras.

En la proposición 1, la hipótesis $\sigma(g) \vee \sigma(h) = 1$ es **esencial.**

En el grupo conmutativo $G, \cdot$ engendrado por el elemento g de orden 4

$$\sigma(g^2) \neq \sigma(g) \vee \sigma(g)$$

12

Cuerpos de Galois

1 – CUERPOS DE GALOIS

DEFINICION

Los cuerpos finitos se llaman **Cuerpos de Galois.**

EJEMPLOS

1. Todos los cuerpos Z_p , + , · (p primo) son cuerpos de Galois.

2. Construiremos el cuerpo F_9 , + , · que comprende $9 = 3^2$ elementos y amplía Z_3 , + , ·

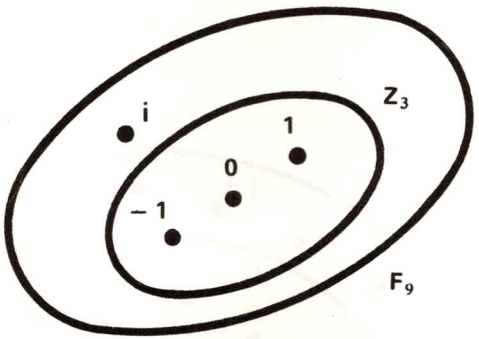


FIG. 81

Se llama i a un elemento de $F_9 \setminus Z_3$

Sea $F_9 = \{ a + b\,i \mid a, b \in Z_3 \}$

Se definen en F_9 una adición y una multiplicación aplicando las reglas corrientes de asociatividad, conmutatividad, distributividad y la regla suplementaria $i^2 = -1$

Es decir, **la adición** y la **multiplicación** en F_9 están **definidas** por

$$\forall\, a, b, c, d \in \mathbf{Z}_3 \quad : \quad \begin{aligned} (a + bi) + (c + di) &= (a + c) + (b + d)\, i \\ (a + bi) \cdot (c + di) &= (a\, c - b\, d) + (a\, d + b\, c)\, i \end{aligned}$$

Es claro que $F_9\ ,\ +\ ,\ \cdot$ es un anillo conmutativo con unidad.

Se sabe que $a, b \in \mathbf{Z}_3 : a^2 + b^2 = 0 \iff a = b = 0$

He aquí $a + bi \in F_9$ (con $a, b \in Z_3$)

Si $a \neq 0$ **o** $b \neq 0$

Entonces $$(a + bi) \cdot \left(\frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}\, i \right) = 1$$

lo cual establece que $a + bi$ es no nulo y que $F_9\ ,\ +\ ,\ \cdot$ es un cuerpo.

En particular, se probó así que

$$\forall\, a, b \in \mathbf{Z}_3 : \quad a + bi = 0 \iff a = b = 0$$

De donde

$$\forall\, a, b, c, d \in \mathbf{Z}_3 : \quad a + bi = c + di \iff a = c \quad \text{y} \quad b = d$$

Luego resulta que F_9 está formado por los siguientes nueve elementos distintos

$$\begin{aligned} 0 &= 0 + 0\, i \\ 1 &= 1 + 0\, i \\ -1 &= -1 + 0\, i \\ i &= 0 + 1\, i \\ -i &= 0 + (-1)i \end{aligned} \qquad \begin{aligned} 1 + i &= 1 + 1\, i \\ -1 - i &= -1 + (-1)i \\ 1 - i &= 1 + (-1)i \\ -1 + i &= -1 + 1\, i \end{aligned}$$

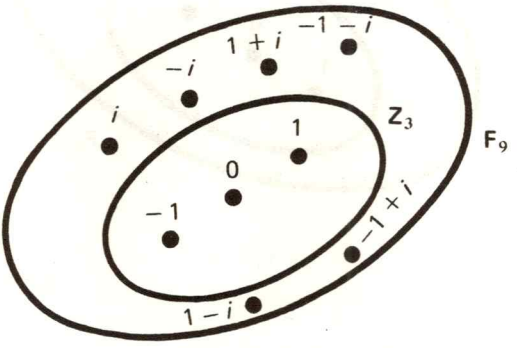


FIG. 82

+	0	1	−1	i	$-i$	$1+i$	$-1-i$	$1-i$	$-1+i$
0	0	1	−1	i	$-i$	$1+i$	$-1-i$	$1-i$	$-1+i$
1	1	−1	0	$1+i$	$1-i$	$-1+i$	$-i$	$-1-i$	i
−1	−1	0	1	$-1+i$	$-1-i$	i	$1-i$	$-i$	$1+i$
i	i	$1+i$	$-1+i$	$-i$	0	$1-i$	−1	1	$-1-i$
$-i$	$-i$	$1-i$	$-1-i$	0	i	1	$-1+i$	$1+i$	−1
$1+i$	$1+i$	$-1+i$	i	$1-i$	1	$-1-i$	0	−1	$-i$
$-1-i$	$-1-i$	$-i$	$1-i$	−1	$-1+i$	0	$1+i$	i	1
$1-i$	$1-i$	$-1-i$	$-i$	1	$1+i$	−1	i	$-1+i$	0
$-1+i$	$-1+i$	i	$1+i$	$-1-i$	−1	$-i$	1	0	$1-i$

TABLA DE ADICION DE F_9

FIG. 83

·	0	1	-1	i	$-i$	$1+i$	$-1-i$	$1-i$	$-1+i$
0	0	0	0	0	0	0	0	0	0
1	0	1	-1	i	$-i$	$1+i$	$-1-i$	$1-i$	$-1+i$
-1	0	-1	1	$-i$	i	$-1-i$	$1+i$	$-1+i$	$1-i$
i	0	i	$-i$	-1	1	$-1+i$	$1-i$	$1+i$	$-1-i$
$-i$	0	$-i$	i	1	-1	$1-i$	$-1+i$	$-1-i$	$1+i$
$1+i$	0	$1+i$	$-1-i$	$-1+i$	$1-i$	$-i$	i	-1	1
$-1-i$	0	$-1-i$	$1+i$	$1-i$	$-1+i$	i	$-i$	1	-1
$1-i$	0	$1-i$	$-1+i$	$1+i$	$-1-i$	-1	1	i	$-i$
$-1+i$	0	$-1+i$	$1-i$	$-1-i$	$1+i$	1	-1	$-i$	i

TABLA DE MULTIPLICACIONES DE F_9

FIG. 84

EJERCICIOS

1. En el grupo multiplicativo $(F_9 \setminus \{0\}), \cdot$

   $\text{grp } 1 = \{1\}$ $\quad\quad$ $\text{grp } (-1) = \{1, -1\}$

   $\text{grp } (i) = \{1, i, -1, -i\} = \text{grp } (-i)$

   $\text{grp } (1+i) = \text{grp } (-1-i) = \text{grp } (1-i) = \text{grp } (-1+i) = F_9 \setminus \{0\}$

2. El grupo $(F_9 \setminus \{0\}), \cdot$ es cíclico.

2 – TEOREMA DE LOS CUERPOS DE GALOIS

1°) El grupo multiplicativo de todo cuerpo de Galois es cíclico.

2°) El producto de elementos no nulos de todo cuerpo de Galois es – 1 (WILSON)

3°) Si K es un cuerpo de Galois tal que $\# K = q$

Entonces $\forall x \in K_0 : \quad x^{q-1} = 1 \quad ; \quad \forall x \in K : \quad x^q = x$ (FERMAT)

4°) Toda transformación de un cuerpo de Galois es una función polinomio de ese cuerpo.

$k_1, \ldots, k_{q-1}$ los elementos no nulos del cuerpo de Galois K (con $\# K = q$)

$$K_0 = \{ k_1, \ldots, k_{q-1} \}$$

DEMOSTRACION DE 3

El grupo K_0 es de orden $q - 1$

$\forall x \in K_0 : \quad x^{q-1} = 1$ (1) (c. 11, t. 5, p. 262)

$\forall x \in K : \quad x^q = x$

l. q. q. d. ·

DEMOSTRACON DE 2

En virtud de 3 , los $k_1, \ldots, k_{q-1}$ son raíces distintas de $"x^{q-1} - 1"$

$"x^{q-1} - 1" = "x - k_1" \cdot \ldots \cdot "x - k_{q-1}"$ (c. 9, t. 3, p. 219)

$\forall x \in K : \quad x^{q-1} - 1 = (x - k_1) \cdot \ldots \cdot (x - k_{q-1})$

$K_0 \to K_0 : \quad k \to -k$ es una permutación de K_0

$\forall x \in K : \quad x^{q-1} - 1 = (x + k_1) \cdot \ldots \cdot (x + k_{q-1})$

En particular, para $x = 0$

$$-1 = k_1 \cdot \ldots \cdot k_{q-1}$$

l. q. q. d.

DEMOSTRACION DE 1

Anotemos

$$n_1 = \sigma(k_1) \ , \ \ldots \ , \ n_{q-1} = \sigma(k_{q-1})$$

$$n = n_1 \vee \ \ldots \ \vee n_{q-1}$$

1°) En virtud de la proposición 2 del capítulo 11 (p. 270) existe un elemento $g \in K_0$ tal que $\sigma(g) = n$

Establecimos en 3 : $g^{q-1} = 1$

Luego, por el teorema 2 del capítulo 11 (p. 262)

$$n \mid q - 1$$

$$n \leqslant q - 1$$

2°) Para todo $i \in \{ 1, \ldots, q - 1 \}$

$$k_i{}^{n_i} = 1 \quad \text{y} \quad n_i \mid n \quad \text{de donde} \quad k_i^n = 1$$

$\forall \ x \in K_0$: $x^n = 1$

La función polinomio "$x^n - 1$" del cuerpo K admite las $q - 1$ raíces distintas $k_1, \ldots, k_{q-1}$

Y, por el teorema 3 del capítulo 9 (p. 219)

$$q - 1 \leqslant n$$

3°) Comparando las fórmulas recuadradas,

$$n = q - 1$$

$$\sigma(g) = \# K_0$$

El elemento g engendra el grupo K_0 , $\cdot$

K_0 , $\cdot$ es cíclico.

l. q. q. d.

DEMOSTRACION DE 4

Se sabe que $[K] \subset K^K$

Como los anillos $[K].=$ y K^K son finitos,

para establecer $[K] = K^K$, basta probar que $\# [K] = \# K^K$

Por una parte, $\boxed{\# (K^K) = \# K^{\# K} = q^q}$

Por otra parte, en virtud de la fórmula de Fermat

$$\forall x \in K : x^q = x \ , x^{q+1} = x^2 \ , \ldots \quad , x^{2q-2} = x^{q-1}$$

$$x^{2q-1} = x \ , x^{2q} = x^2 \ , \ldots, \text{ etc.}$$

Toda función polinomio de K se escribe

$$"a_{q-1} x^{q-1} + \ldots + a_1 x + a_0" \quad \text{donde los} \quad a_i \in K$$

y está definida por la sucesión $a_{q-1}, \ldots, a_1, a_0$ de q elementos de K

Como el cuerpo K comprende k elementos, el teorema 4 del capítulo 9 (p. 221), prueba que dos de estas sucesiones distintas definen polinomios diferentes.

Existe, por lo tanto, una biyección

$$[K] \rightarrow K^q$$

del anillo de funciones polinomios [K] sobre el conjunto K^q de sucesiones de q elementos de K

Luego $\# [K] = \# (K^q) = (\# K)^q = q^q$

$$\boxed{\# [K] = q^q}$$

Comparando las fórmulas recuadradas

$$\# [K] = \# (K^K)$$

l. q. q. d.

EJERCICIOS

Si F es un cuerpo finito de cardinal q

Entonces $F \setminus \{0, 1\}$ es el conjunto de raíces de la función polinomio "$x^{q-2} + x^{q-3} + \ldots + x^2 + x + 1$"

INDICE

INDICE

pág.

anillos de restos o anillos residuales 164
asociatividad mixta 190
característica (función—) 10
clases laterales de un subgrupo 236
clase lateral derecha 237
izquierda 237
combinación lineal 59
cuerpos de Galois 273
(teorema de los—) 277
cuerpos residuales 170
distributivo (reticulado—) 131
divisor (más alto común—) 84
divisores de una parte 76
divisores de cero 168
epimorfismo 178
estable para la adición 53
la sustracción 53
Euclides (teorema de—) 225
exponente 188
factorial 16
factorización prima 102
Fermat (teorema de—) 176
fracciones parciales 143
función característica 10
función polinomio 206
Galois (cuerpos de—) 273
grado de una función polinomio ... 225
idempotente de un grupo 233
isomorfismo 178
Lagrange (teorema de—) 244

pág.

laterales (clases—) 236
más alto común divisor 84
más bajo común múltiplo 92
módulo de una parte 59
morfismo 178
Newton (fórmula de—) 42, 191
números naturales primarios 111
orden de un elemento de un grupo . 258
grupo 244
Pascal (fórmula de—) 28
(triángulo de—) 31
polinomio (función—) 206
potencia 188
potencias en un grupo multiplicativo 150
prima (factorización—) 102
primarios (números naturales—) ... 111
primo (entero racional—) 97
primos entre sí (enteros racionales) 95
raíces de una función polinomio .. 218
reticulado 128
distributivo 131
Stone (teorema de—) 122, 135
subgrupo de Z, + engendrado por una parte 61
un entero racional 63
Wilson (teorema de—) 223

TABLA DE MATERIAS

TABLA DE MATERIAS

pag.

LIBRO 1

COMBINATORIA

CAPITULO 1 . Combinatoria

1. Problema 3
2. Producto de varios conjuntos 4
3. Número de aplicaciones del conjunto finito A en el conjunto finito B 6
4. Número de partes de un conjunto 10
5. Número de inyecciones del conjunto finito A en el conjunto finito B 13
6. Biyecciones y permutaciones 16
7. Número de partes de p elementos de un conjunto finito de n elementos 21
8. Propiedades de $\binom{n}{p}$ 24
9. Triángulo de Pascal 26
   PASCAL 37
10. Fórmula de Newton 38
11. Número de sucesiones de p números naturales cuya suma es n 43
    NEWTON 49

LIBRO 2

LA ARITMETICA DE LOS NUMEROS ENTEROS RACIONALES

CAPITULO 2. **Subgrupos de Z, +**

1. Partes de Z' + estables para la adición, partes de Z, + estables para la sustracción 53
2. Subgrupos de Z, + engendrados por una parte P de Z 58
3. Subgrupos de Z, + engendrados por un entero racional 58
4. Subgrupos de Z, + ... 65

CAPITULO 3. **Más alto común divisor**
Más bajo común múltiplo

1. La relación "divide" en Z 69
2. Conjunto de divisores de una parte de Z 76
3. Comparación de los órdenes $\leqslant$ y $|$ definidos sobre ω_0 80
4. Más alto común divisor 82
5. Cálculo del más alto común divisor de una cupla de enteros racionales 86
6. Más bajo común múltiplo 92

CAPITULO 4. Factorizaciones primas de los números naturales

1. Enteros racionales primos entre sí 95
2. Enteros racionales primos 97

CAPITULO 5. $\omega, \Lambda, \vee, |$

1. M.A.C.D. , M.B.C.M. y factorizaciones primas 107
2. Números naturales primos 111
3. Isomorfismo $q : \omega, | \to \Phi \subset$ 117
4. Isomorfismo $q : \omega, \Lambda, \vee, | \to \Psi \cap' \cup' \subset$ 121
5. Propiedades de $\omega, \Lambda, \vee$ 124
STONE 127
1. Reticulados 128 128
2. Reticulados distributivos 131

LIBRO 3

LA ARITMETICA DE LOS NUMEROS RACIONALES

CAPITULO 6. La aritmética de los números racionales

1. Números racionales 139
2. Fracciones parciales 141
3. La relación . . . divide . . . definida en Q 144
4. Factorizaciones primas de los números racionales 146
5. M.A.C.D. y M.B.C.M. de cuplas de racionales 150
6. Subgrupos de Q, + ... 154

LIBRO 4

ANILLOS CONMUTATIVOS Y CUERPOS

CAPITULO 7. Anillos y cuerpos residuales

1. El anillo $Z_n, +, \bullet$ 159
2. Divisores de cero 168
3. Cuerpos residuales 168
4. Ejercicios 171
5. El cuerpo $Z_n, +, \bullet$ 174
6. Morfismos 178
FERMAT 181

CAPITULO 8. Anillos conmutativos y cuerpos

1. Anillos conmutativos, con unidad y cuerpos 183
2. Cero es absorbente 184
3. Regla de los signos 185

4. Multiplicación escalar 186
5. Potencias en un anillo 188
6. Una nueva asociatividad mixta 188
7. Dos fórmulas importantes 191
8. En los cuerpos no hay divisores de cero 192
9. Potencias con exponentes enteros racionales de elementos no nulos de un cuerpo 193
10. Ejercicios 195
11. El anillo de aplicaciones de un conjunto E en un anillo A, +, • 197

CAPITULO **9. Funciones polinomios de un anillo**

1. Funciones polinomios de un anillo 206
2. Anillo de funciones polinomios de un anillo 210
3. Divisibilidad por "$x - a$" 213
4. Raíces de las funciones polinomios 218
5. Expresión única de ciertas funciones polinomios 221
6. Teorema de Wilson 223
7. Grado de una función polinomio de un cuerpo infinito 225
8. Ejercicios 226

LIBRO 5

PROPIEDADES ARITMETICAS DE LOS GRUPOS Y CUERPOS DE GALOIS

CAPITULO **10. Subgrupos de un grupo**

1. Subgrupos 233
2. Clases laterales del subgrupo 5Z de Z, + ... 235
3. Clases laterales de un subgrupo de G, * 237
4. Orden de un grupo y de sus subgrupos 244
   LAGRANGE 247

CAPITULO **11. Orden de los elementos de un grupo**

1. Potencias en un grupo multiplicativo 249
2. Subgrupo engendrado por un elemento 253
3. Orden de un elemento de un grupo 258
4. Potencias de los elementos de orden infinito de un grupo 264
5. Orden y producto 269

CAPITULO **12. Cuerpos de Galois**

1. Cuerpos de Galois 273
2. Teorema de los cuerpos de Galois 277

La EDITORIAL UNIVERSITARIA S. E. M., dio término a la impresión de esta obra en el mes de setiembre de 1971, en los Talleres Gráficos de Pablo Paoppi e Hijos S. A., Santo Domingo 2265, Buenos Aires.

está acompañado de una serie de interesantes ejercicios programados.

Si bien los temas expuestos en esta obra son de gran trascendencia en la matemática moderna, su mérito fundamental consiste en el uso de recursos pedagógicos novedosos que hacen más accesible la materia. Los esquemas multicolores, los ejemplos inspirados en la vida cotidiana, las demostraciones mediante films, la simplicidad que domina toda la obra, son medios didácticos de gran valor, compatibles con el más severo rigor matemático.

Georges Papy se doctoró en matemática en la Universidad de Bruselas y pronto enseñó allí y en otras universidades extranjeras. Consagrado a la reforma de la enseñanza de la matemática en la escuela secundaria, desde 1961 dirige el Centro Belga de Pedagogía de la Matemática.

ALGUNOS TÍTULOS DE EUDEBA

La enseñanza de la matemática moderna en el primer curso - C. A. Trejo y J. E. Bosch

Ciclo medio de matemática moderna - C. A. Trejo y J. E. Bosch

Álgebra para escuelas secundarias - O. Varsavsky

Introducción al álgebra, nociones de álgebra lineal - M. Cotlar y C. Ratto de Sadosky

Introducción a la teoría de conjuntos - L. Oubiña

EDITORIAL UNIVERSITARIA DE BUENOS AIRES